FRONTEX

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

Research and Development Unit

Last reviewed on
31/08/2012

Version 2.0
Status: APPROVED

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

www.frontex.europa.eu
Rondo ONZ 1, 00-124 Warsaw, Poland
Tel. +48 22 205 95 00
Fax +48 22 205 95 01

TABLE OF CONTENTS

LEGAL NOTICE

The contents of this publication do not necessarily reflect the official opinions of any institution or body of the European Union. Neither Frontex nor any person or company acting on behalf of Frontex is responsible for the use that may be made of the information contained in this report.

ALL RIGHTS RESERVED

Before using the Frontex Best Practice Technical Guidelines for Automated Border Control (ABC) Systems:

1. Please contact the Frontex Research & 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 is 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 & Development Unit contact data at the end of the document

For the above purposes, please use information below.

Latest releases at the time of writing:

"Best Practice Operational Guidelines for Automated Border Control Systems", v 2.0, August 2012.

"Best Practice Technical Guidelines for Automated Border Control (ABC) Systems", V 2.0, August 2012.

Frontex RDU contact data:

Rasa Karbauskaite
Research and Development Unit
Capacity Building Division
Frontex
Rondo ONZ 1, 00-124 Warsaw, Poland
Tel: +48 22 205 96 25
Fax: +48 22 205 95 01

Ignacio Zozaya
Research and Development Unit
Capacity Building Division
Frontex
Rondo ONZ 1, 00-124 Warsaw, Poland
Tel: +48 22 205 95 70
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 a number of border crossing points of the European Union. Frontex would like to particularly acknowledge the work of the following persons, who participated in the Working Group on Automated Border Controls:

- Finland: Alapelto Pentti, Max Janzon and Pasi Nokelainen (Finnish Border Guard).
- France: Dominique Gatinet (French Secure Documents Agency), Laurent Mucchielli (Border Police).
- Germany: Markus Nuppeney (Federal Office for Information Security) and Maik Rudolf (Federal Police).
- Netherlands: Yvonne Bakker, Kier-co Gerritsen, Joost van Aalst (Ministry of Justice), and Rijck van de Kuil (Royal Netherlands Marechaussee).
- Portugal: Paula Maria Azevedo Cristina and Maria Conceição Bértolo (Immigration and Border Service).
- Spain: Javier Núñez Alonso (Spanish National Police) and Ángel L. Puebla (Spanish National Police).
- United Kingdom: Andrew Clayton, Daniel Soutar and Glen Wimbury (UK Border Agency).

In addition, the following staff from the Frontex RDU participated in the drafting and editing process: María Duro Mansilla, Rasa Karbauskaite, Gustav Soederlind and Ignacio Zozaya.

Frontex is also grateful to other stakeholders who contributed to the review process.

ABOUT FRONTEX RESEARCH AND DEVELOPMENT UNIT

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.

The core objective of the Capacity Building Division is to drive process of harmonisation and standardisation, promoting 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 for the control and surveillance of external borders and keeps the Member States and the European Commission informed concerning technological innovations in the field of border control. In particular, one of RDU 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.

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

ACRONYMS AND ABBREVIATIONS

AA	Active Authentication
ABC	Automated Border Control
B900	IR sensitive ink
BAC	Basic Access Control
BCP	Border Crossing Point
BMP	Image format Windows Bitmap v3
BPG	Best Practice 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)
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)
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)
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
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 (global standard)
EU	European Union
EU/EEA/CH	European Union, European Economic Area, Switzerland
FAR	False accept rate
FRR	False reject rate
FTC	Failure-to-capture
ICAO	International Civil Aviation Organization
ID	Identity Document
IR	Infrared light
IS	Inspection System
ISO	International Organization for Standardization
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)
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, redirect travellers as required (for example, to second line checks), and assist them on 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 e-MRTD, establishes that the passenger is the rightful holder of the document, queries border control records and automatically determines eligibility for border crossing according to 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 Verification: The process of confirming the identity of the holder of an e-MRTD by the measurement and validation of one or more unique 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 authorized to enter the territory of the Member States or authorized to leave it. See also *"Border Crossing Point (BCP)".*

Border Crossing Point (BCP): Any crossing-point authorized 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 the immediate vicinity of that border who carries out, in accordance with the Schengen Borders Code and national law, border control tasks.

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 the present 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 to 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).

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.

---

[2] The definitions including 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 reference list in Annex I). Finally, a number of definitions have been devised and agreed by the Frontex Working Group on Automated Border Controls.

Customer Service Personnel: Within the context of the present Best Practice Guidelines, the term refers to the staff of the port operator which is 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 which 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".*

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

e-Gate: One of the components of an ABC system, consisting of a physical barrier operated by electronic means.

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

e-Passport : 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 cryptographic technology, and which conforms to the specifications of 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 Capture: The failure of a biometric system to obtain the necessary biometric to enroll 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 enrollee or verify the legitimate claimed identity of an enrollee. 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 enrollee identification attempts, and NEVA is the number of enrollee verification attempts. This estimate assumes that the enrollee identification/verification attempts are

representative of those for the whole population of enrollees. The false rejection rate normally excludes "failure to acquire" error.

First Line Check: 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 a biometric match 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 sub-system components to work together.

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

Member State: A country which is member of the European Union. Within the context of the present 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 autocorrection 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.

Multibiometrics: 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 one 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) monitor the user interface of the application; b) react upon any notification given by the application; c) manage exceptions and make decisions about them; d) communicate with the assisting personnel for the handling of exceptions at the e-Gates; e) monitor and profile travellers queuing in the ABC line and using the e-Gates looking for suspicious behaviour in travellers; and, f) communicate with the border guards responsible for second line checks whenever their service is 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 unforged by tracing it back to the Country Signer Certificate Authority (CSCA) certificate of the issuing country. See also *"Active Authentication".*

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 which operates the port facility, either at 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, Cyprus, Ireland, 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 which 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 verifies 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 *"Segregated Two-Step Process".*

Service Level Agreement (SLA): A 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.

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.

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".*

PREAMBLE

Despite economic uncertainties, traveller's traffic at the EU airports rose 4.8 per cent in 2011 compared to 2010 levels. This trend is predicted to continue over the next 20 years, with global traffic growing some 6 per cent annually.[3] At the policy level, facilitating access to Europe in a globalised world constitutes one of the strategic goals of the European Union for the further development of the area of freedom, security and justice.[4] The aim is to continue easing access to the Union's territory for those having a legitimate interest, while at the same guaranteeing high level of security for EU citizens.

Yet, as traveller numbers continue to rise, it can be expected that the current infrastructure at international border crossing points will have greater difficulties in dealing with increased throughput. The dual objective of facilitating travel and maintaining security requires of the introduction of new approaches and innovative solutions to border management. The installation of Automated Border Control (ABC) systems at a number of European airports constitutes an integral part of this effort.

While the rollout of ABC systems has expanded over recent years, it has so far taken place in a disconnected manner. As ABC solutions are relatively immature, there is a need for a coordinated and detailed exchange of experiences and lessons learnt regarding the benefits and challenges of such automation. Since 2010 Frontex has undertaken a number of initiatives to further develop and identify best practices and guidelines on ABC. The objective is to help fill the current knowledge gap, with a view to increase the efficiency and effectiveness and to harmonise user experience of checks at the EU external borders.

The establishment of a Working Group on ABC, composed of experts from Member States' border management authorities, has been one of such initiatives. The Working Group was tasked with the elaboration of minimum technical and operational requirements for ABC systems. This experience resulted in the publication of the Frontex Release 1.1 of the "Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems" in March 2011. The Guidelines set out the basic "blueprint" of an ABC system and succeeded in creating vast interest among Member States and other stakeholders.

In July 2011 the Working Group was reactivated with a view to upgrade the Best Practice Guidelines on the basis of the feedback received from the relevant community, and to account from the introduction of new technologies as well as for changes in practice. Importantly, the Working Group decided to address the technical and operational dimensions of ABC systems in different documents in order to give greater entity to both categories of issues and to better target distinct audiences. The outcome of this coordinated effort is constituted by the present Best Practice Technical Guidelines and their complementary resource, the ABC Best Practice Operational Guidelines for ABC Systems.

The current documents are intended to be living ones. In this respect, Frontex would like to benefit from the input and expertise of relevant stakeholders in the field of ABC, such as national border management authorities, policy makers, international organizations, standardisation bodies, port authorities, academia, and industry offering technologies and products related to ABC. Future plans also include enlarging the set of requirements towards making facilitated border crossing accessible to a larger group of eligible persons, in particular third country nationals, and continue the development of a comprehensive roadmap for automated border controls. In doing this, Frontex will strive to promote closer cooperation with international organisations and standardisation bodies which are currently undertaking initiatives in this area, in order to ensure that a vision is shared among the stakeholders responsible for shaping the future of automated border control.

Edgar Beugels
Head of the Research and Development Unit

[3] *Boeing, "Current Market Outlook 2012-2031 – Long Term Market", 2012.*
[4] *As established in the Stockholm Programme for the period 2010-2014*

EXECUTIVE SUMMARY

The present 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. **Automated Border Control (ABC)** is defined as the use of automated or semi-automated systems which can verify the identity of travellers at border crossing points (BCPs), without the need for human intervention. The term **Best Practice Guidelines (BPG),** on the other hand, refers to knowledge, typically based on experience, which can be shared in order to achieve improved results towards specific objectives.

These BPG 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** are technical experts involved in the design and implementation of ABC systems in the EU Member States (MSs), including project managers and system architects from border management authorities. While these ABC Best Practical Technical Guidelines have been conceived as a standalone resource, ideally they should be read in combination with the Frontex "Best Practice Operational Guidelines for ABC Systems".

Both documents focus 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 of pre-enrolment. Registered Traveller Programmes (RTPs) are outside its scope. The **biometric markers** covered include both facial recognition and fingerprints.

The BPG 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 match 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 which are scratch proof and impact-resistant. The system must also be constructed in such a way so as 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 or double 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. 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 database should be kept up to date in order to y avoid significant increases of 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/datagroups from e-Passports: EF.COM, EF.SOD, 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 Basic Access Control (BAC), 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. D**ocument verification** is mainly covered by the Passive Authentication (PA) security method, the reliability of which is guaranteed only of trustworthy Document Signer (DS) certificates and Country Signing Certification Authority (CSCA) certificates are applied. Thus, a trusted certificate store should 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; 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 (DG1 vs. 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 which support their national e-ID cards.

Biometric verification

Biometric verification is the process whereby, by 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.

The biometric verification process is 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.

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 flow of the traveller 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 at least 0.001 (0.1 per cent). At this configuration the 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 upon request by the operator.

On the other hand, the use of two or more biometric modalities may be incorporated in national ABC implementations. **Multibiometrics** allow for better results than a process based on a single biometric, reducing the risk of false positives and negatives. Several types of multibiometrics 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 [ISO24722].

Quality control

Quality control 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, ensure that it meets the expectations of travellers and border management authorities.

The BPG focus on the **minimum recommended anonymous operational data** to be collected for quality control and the extraction of business statistics in ABC systems. The data stored should include at least information on the following types of transactions: access attempts with documents not accepted by the system (i.e. non-electronic passports, not a passport); access attempts with non-eligible documents (i.e. underage Schengen citizens holding an e-Passport, third country nationals holding an e-Passport); and access attempts by an eligible traveller, with a valid e-Passport but whose verification was not successful (for example due to a biometric verification error). Importantly, the collection and storage of data should comply with the limitations imposed by EU and data protection regulations. 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 further, manual, action required by the officers monitoring the BCP. Data entries should include information on the nationality of the document issuer, and the travellers' age and gender. The

total verification time and the access time (the total time spent by an eligible traveller in the process since its 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 having a continuous quality control, the extraction of business statistics and the introduction of improvement 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 be stored as well on those background checks.

Finally, for the purposes of quality control, each ABC installation, a 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 present terminology 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", mean that the definition is an absolute requirement.
SHALL NOT	This phrase, or the phrase "MUST NOT", mean that the definition is an absolute prohibition.
SHOULD	This word, or the adjective "RECOMMENDED", mean 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" mean 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", mean 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.

1. INTRODUCTION

1.1. Purpose and Audience

This document presents a compendium of best practice guidelines on the technical design of automated border control (ABC) systems. These have been elaborated in an effort to achieve 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 (BCPs) of the European Union (EU) 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 (MSs). Project managers and system architects from border management authorities will find detailed technical information in order to specify and implement a system that performs up to standards while staying away from previously known risks and dead-end streets. In addition, 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.

1.2. Scope and Methodology

The scope of the present document is aligned with the European Commission (EC) and the International Civil Aviation Organisation (ICAO) recommendations, as available at the time of writing, on the use of e-Passports for automated border control without enrolment.[5]

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 shape of Registered Traveller Programmes (RTPs). 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 1st and 2nd generation e-Passports.[6] There are no specific provisions in this document for combined or stand alone 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 2nd 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.

Methodology

The methodology used by the Working Group (WG) to develop the Best Practice Guidelines set out in this document was based on the following tasks:

- State the problem and goals.
- Elaborate the list of relevant topics to be covered.

[5] *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, 13.02.2008; ICAO, "Guidelines for electronic – Machine Readable Travel Documents & Passenger Facilitation", Version – 1.0, 17.04.2008.*

[6] *ICAO ("Doc 9303 Machine Readable Travel Documents", Third Edition 2008]) defines 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) contain also two fingerprints in addition to the facial image.*

- 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 present document.
- Conduct an internal and external review of the document.
- Approve these guidelines.

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

A best practice is a technique, method, process, activity, incentive, or reward which conventional wisdom regards as more effective at delivering a particular outcome than any other technique, method, process, etc. when applied to a particular condition or circumstance. The rationale behind this is that with proper processes, checks, and testing, a desired outcome can be delivered with fewer problems and unforeseen complications. A given best practice may be only applicable to a particular condition or circumstance and will typically need to be modified or adapted for similar but different circumstances.

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 a mandatory procedure). Guidelines may be issued by and used by any organization (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 many times they are used together. Thus the term Best Practice Guidelines has been widely adopted in the industry to reflect that knowledge, typically based on experience, which can be shared in order to achieve improved results towards specific objectives. Along the present document, the term Best Practice Guidelines (BPG) will be used.

1.4. How to Read This Document

While the ABC Best Practice Technical Guidelines have been conceived as a standalone 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 "BPOG").

The present 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.
- Quality control aspects of ABC systems.

A clarification of the terminology used, a glossary and a list of acronyms 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 an overview of the ABC systems which are operational and planned in the EU.

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 whom the travel document claims to be, c) the traveller is eligible to enter the country, and lastly d) the traveller does not pose a threat to its citizens or institutions. With the improvement of technology applied to forging documents, the use of aliases and look-alikes, and the time pressure associated to 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 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.[7] 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 authorized parties can access the information contained inside. 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.[8]

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 authorization to cross the border at a BCP without the need for human intervention.

3. ARCHITECTURE OF AN ABC SYSTEM

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

- Physical barriers (one or two e-Gates).
- Monitoring and control station and equipment for the operator.
- Document reader (optical devices including Radio Frequency (RF) reader module).
- 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 BPOG on "Topologies of ABC system"):

[7] *ICAO, "Doc 9303 Machine Readable Travel Documents", Third Edition 2008.*

[8] *Under 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.*

One-step ABC system

- The traveller is able to complete all transactions 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 the 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 sections 4 on "the document authentication process" and 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 which caters for all users. A smooth passage of the ABC system 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 amongst others the need for drilling, mounting of additional barriers, and wiring requirements (power and data).

3.2. Security & 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 or through the ABC system.

This is typically achieved by the usage of single or double e-Gates and tailgating detection/prevention mechanisms, or by operating the system in a secure area. Typically a 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 force so as to cause injury to the traveller. Other moving parts (e.g. 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 and 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 -[9] presented by the traveller is checked in order to determine whether it is a genuine one which enables 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 realized in software) 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.

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

4.1. Requirements on the document reader

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 that the market may provide for regarding document readers.

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 right as well as 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 in lengthwise orientation, i.e. with the biographical data page facing down and the MRZ-side first towards the document reader.

The document reader SHALL have an integrated RF module according to [ISO14443] 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).

[9] *Concerning the use of alternative e-MRTDs see section 4.6.*

The document reader SHALL have a dedicated wired connection as physical interface to a host system (e.g. 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 which 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.

The document reader SHOULD have a proper shielding against interfering of external light.

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

4.1.2. Capability requirements

ABC systems SHOULD use 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. In average, optical images of the biographical data page SHOULD be captured within two seconds, and reading of the electronic data (at least EF.COM, EF.SOD, DG1 and DG2) from a typical 1st generation e-Passport SHOULD NOT take more than eight 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 optical 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 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 (VIZ).

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 which consists 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 which allows for maintenance and support by the operating agency itself or by a trusted third-party provider under a contract with and the supervision of the operating agency. The usage of a pattern database that does not allow for modifications of the database content by the operating agency (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/datagroups from e-Passports: EF.COM, EF.SOD, 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 the security protocols Basic Access Control (BAC), Active Authentication (AA) and Chip Authentication (CA). 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 proven knowledge of 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 DV – an organizational 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 IS.

Further details on EAC are given in [BSI03110].

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

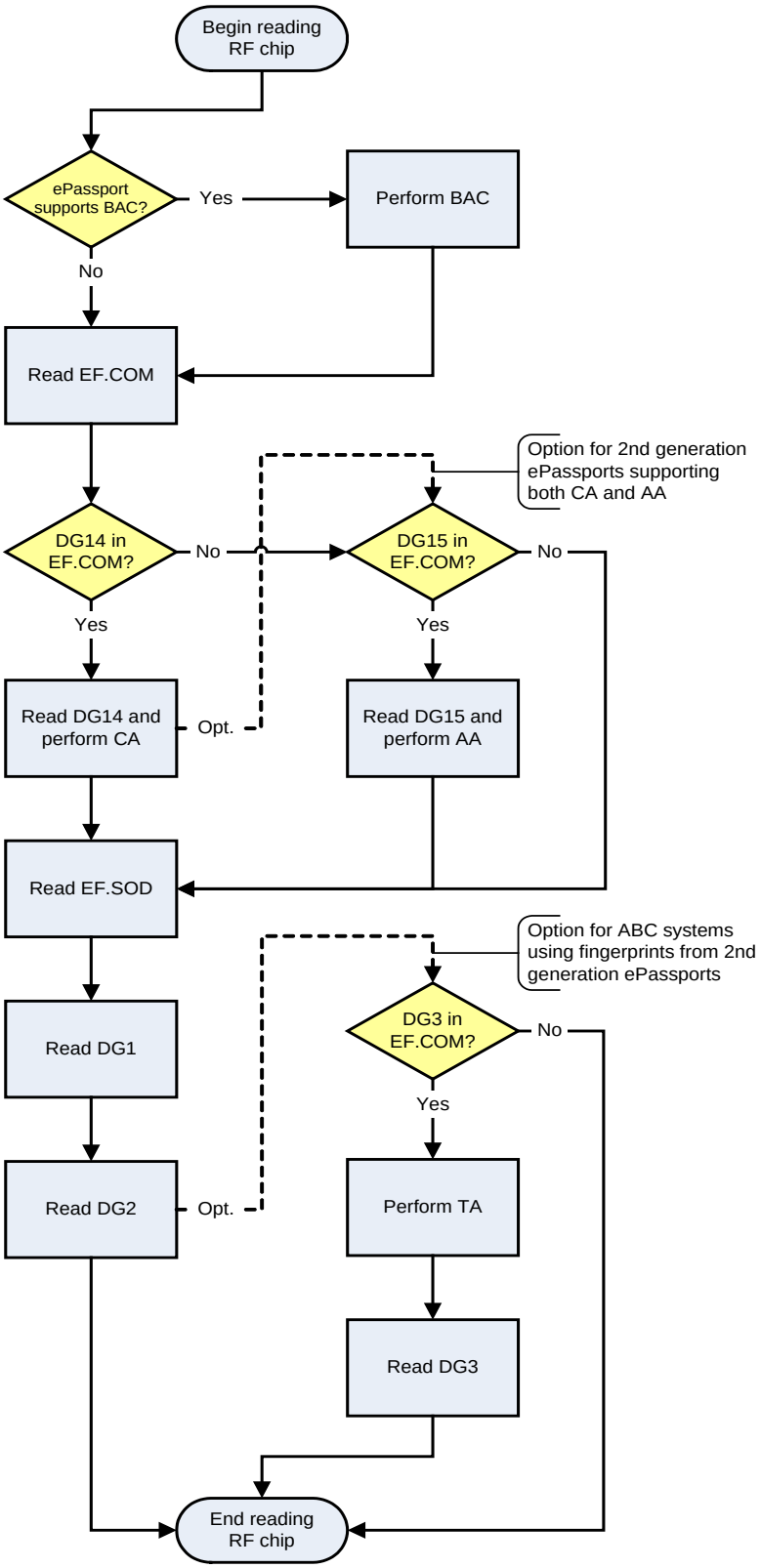


Figure 1: High-level sequence for RF chip reading

4.4. Verification of e-Passport data

Once the e-Passport chip has been read, ABC systems MUST verify the data. Such e-Passport data verification process is mainly covered by the Passive Authentication (PA) security method defined by [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. 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 can not be depended upon and is thus rendered useless. Therefore, the ABC system MUST be provided with certificates from a trusted certificate store.

It is RECOMMENDED to implement this trusted certificate store as a centralized 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 for assuring the integrity and authenticity locally on each client ABC system can be saved. As an add-on when implementing a centralized trusted certificate store, sub-steps 2, 3 and 4 of the PA procedure (see below) MAY be implemented as a centralized 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.
6. Datagroup 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:

a. Comparison of optical and electronic biographical data (DG1 vs. MRZ).
b. 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 if one or more of the particular sub-steps 4.4.1 – 4.4.8 (see details below) end up with the result "Failed".

During the PA procedure additional information about DS certificates or datagroups (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 [ICAO9303] as a SignedData 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. [ICAO9303] provides that the DS certificate MAY be included in EF.SOD. In practice, most countries are issuing e-Passports which 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 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 datagroup 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 AuthorityKeyIdentifier extension from the DS certificate and search for a CSCA certificate with the corresponding value in its SubjectKeyIdentifier extension. Although the usage of these extensions is specified as mandatory by [ICAO9303], there are some countries which 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 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 certificate revocation information, the result of this sub-step MUST 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 can not be detected by just verifying the signature of the EF.SOD. Thus, ABC systems SHALL compare the content of EF.COM with EF.SOD to make sure 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. Datagroup integrity check

For each datagroup that was read from the e-Passport chip, ABC systems MUST calculate the datagroup's digest (hash-value) and compare it with the corresponding digest contained in EF.SOD. ABC systems SHALL rely on the content of a datagroup 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 datagroup (DG14 in case of CA and DG15 in case of AA).

If all of the performed datagroup 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 to perform 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".

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 another country 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.
  Note: 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.

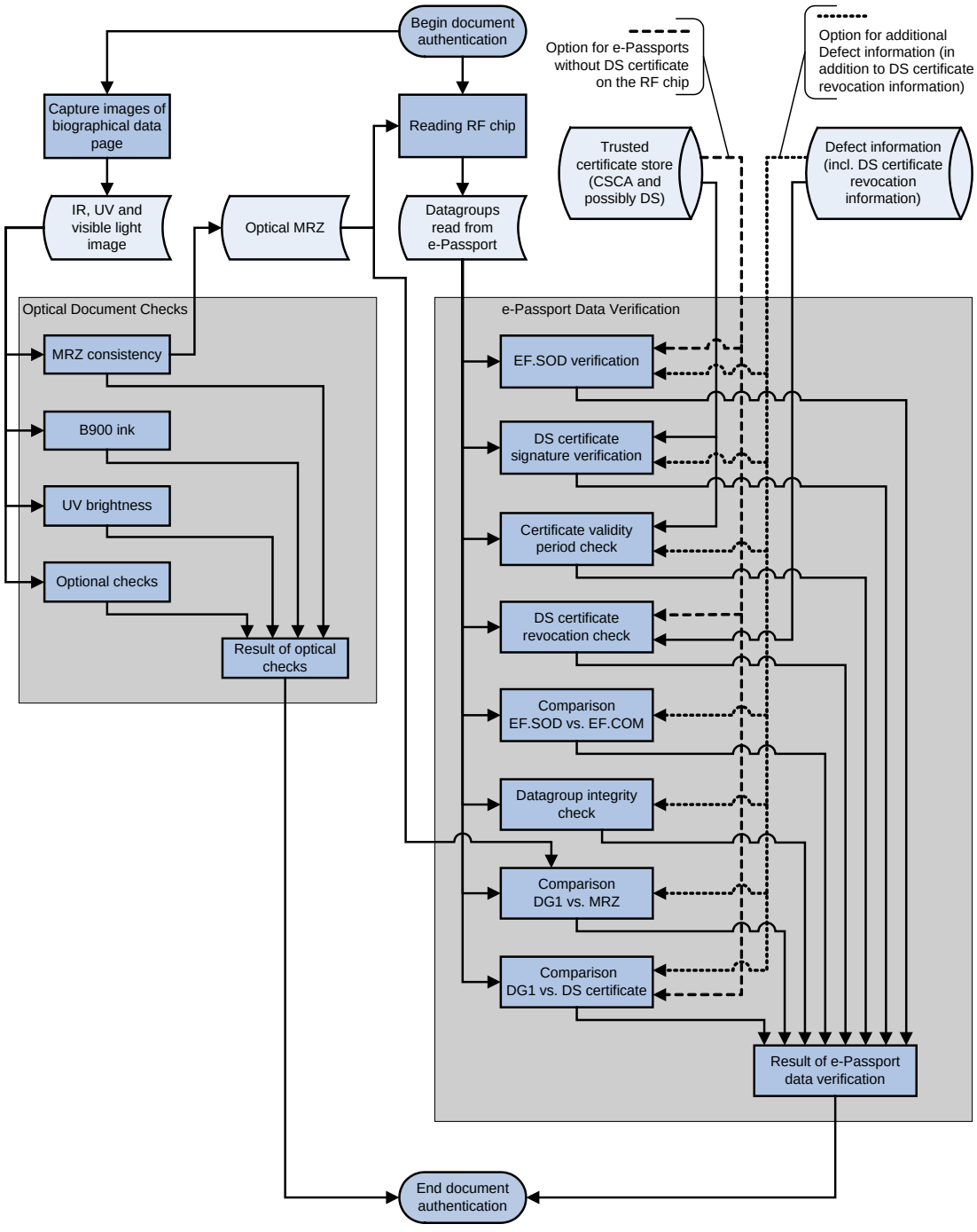
It is RECOMMENDED to use such Defect information about erroneous e-Passports during the process of e-Passport data verification.

4.5. Design of the Document Authentication Process

There are several interdependencies amongst 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 datagroup, etc.) is available. Performing these steps concurrently (that is, running several tasks in parallel) as much as possible allows for a minimization of the time period required for the entire document authentication process.

A high-level illustration of the RECOMMENDED document authentication process for ABC system is shown in Figure 2.

Figure 2: Document authentication process



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 in the discretion of the MSs to decide if and what kinds of alternative e-MRTDs 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 the validation of the document and for access to its protected data areas.

Currently a number of approaches to national ID cards with biometric capabilities are in the field. At the time writing, Germany and Spain had ABC implementations supporting e-ID cards:

Details on both systems are included below, for illustration purposes, as specific case studies.

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 3: German electronic ID card (front and back)

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.
- QES application for doing qualified electronic signatures.

For use within the context of border control 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 given in [BSI03121].

The main difference between the e-ID card and the e-Passport lays in the protection of the stored data from unauthorised access. While for EU e-Passports DG1 and DG2 are protected by BAC (Basic Access Control) 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 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.

The IS used by the German Federal Police to verify ID cards and e-Passports follows a distributed approach. A Terminal Control Center [BSI03129] (TCC) offers a central service that connects the distributed readers (for example, those which are part of an ABC system). The TCC supports different application scenarios for BAC and EAC protected documents. A secure centralised key and certificate storage is 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:

	EU e-Passport (ID3 size)	**German 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
CAN	not available	printed on front side of ID card
Electronic data		
DG1 (MRZ data)	mandatory	mandatory
DG2 (face image)	mandatory	mandatory
DG3 (fingerprint images)	mandatory	optional
Access control	BAC (DG1, DG2) EAC1 (DG3)	PACE with EAC2 (all DGs)

Table 1: Comparison of e-Passport vs. German electronic ID card

Since August 2011 the EasyPASS ABC system in Germany is 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.

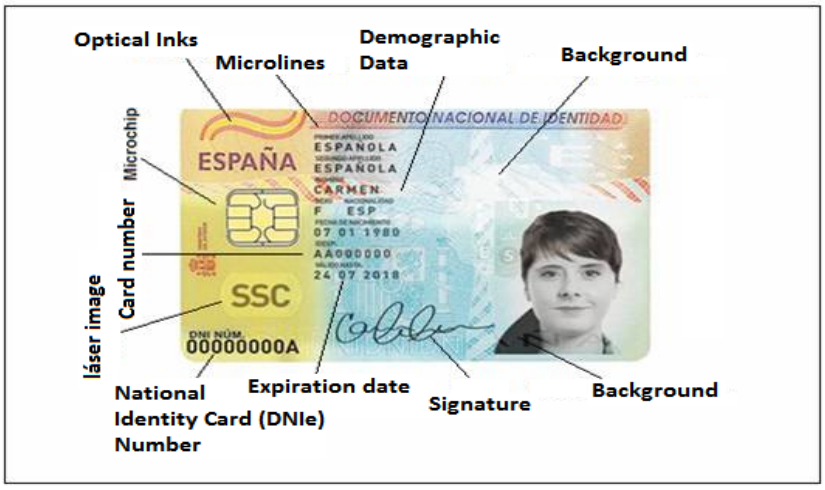


Figure 4: Spanish electronic ID card (front)

Figure 5: Spanish electronic ID card (back)

The chip of the ID card contains two different applications:

- Match-on-card biometric application ([ISO7816-11] compliant) using fingerprints patterns ([ISO19794-2] compliant).
- Application for recognized electronic signatures.

The data are stored in the biometric application in [ISO19794-2] 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 ABC systems other than the Spanish one.

The interface of the match-on-card software is compliant with [ISO7816-11] standards.

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

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

	EU e-Passport (ID3 size)	**Spanish 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 (ICAO compliant)
Electronic data		

(MRZ data)	Mandatory (DG1 format)	Mandatory (raw format)
(face image)	Mandatory (DG2 format)	Mandatory (ISO 19794-5)
(fingerprint images)	Mandatory (DG3 format)	Mandatory (ISO 19794-2)
Access control	BAC (DG1, DG2) EAC1 (DG3)	Securized by CWA 14890 Protection profile CWA 14169

Table 2: Comparison of e-Passport vs. Spanish electronic ID card

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

5. THE BIOMETRIC VERIFICATION PROCESS

Biometric verification is the process whereby, by using biometric technology, it is verified that the person holding the e-MRTD is actually the owner of the e-MRTD.

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 [ICAO9303] 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 that the market may provide for regarding biometric capture and verification.

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 flow of the traveller (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 [ISO19794-5]. 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 SHALL 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 in times where no face images are captured. Sunlight will vary both on a daily and on a seasonal basis. It is RECOMMENDED to test that the system will perform adequately under different sunlight conditions. It is RECOMMENDED that direct sunlight is avoided, and environmental illumination

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

The face capture unit SHOULD give feedback to the traveller by an integrated display. It is RECOMMENDED to show the live stream that is currently captured (digital mirror) and to give an indication if the image is 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 standard state of the art interfaces (e.g. USB2.0, Ethernet, FireWire) SHALL be used.

It is RECOMMENDED to use standard interfaces according to BioAPI [ISO19784-1] for the capturing of 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. The pre-processing SHOULD cover at least

- 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 according to [ISO19794-5]. 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 [ISO19794-5]). 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 one second per frame.

5.1.2. Face Verification Unit

5.1.2.1. 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.

5.1.2.2. 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 error rate of about 10 per cent. Thus, this additional check may raise an alert for 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 one second.

The configuration of the face verification algorithm SHALL ensure a security level in terms of the False Accept Rate (FAR) of at least 0.001 (0.1 per cent). 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 on the standard configuration of 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.

Note: 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 follows:

- The reference face images (DG2 images) of the last ten e-Passport verifications are temporarily and anonymously stored in a dynamic list.
- The live face image from the actual face verification process is compared against all other faces in the dynamic list and the comparison scores are saved (impostor

comparisons). It 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 to the applicable data protection regulations.
- Calculate the FAR based on the impostor comparison scores. Genuine comparison scores MAY be used to calculate the corresponding FRR. Care has to be taken about the statistical base for the FAR calculation. In order to measure the performance of the face verification algorithm up to a security level (FAR) of 0.001 (0.1 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 for looking 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 draw off 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 be displayed upon request by the operator of the ABC system.

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 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.

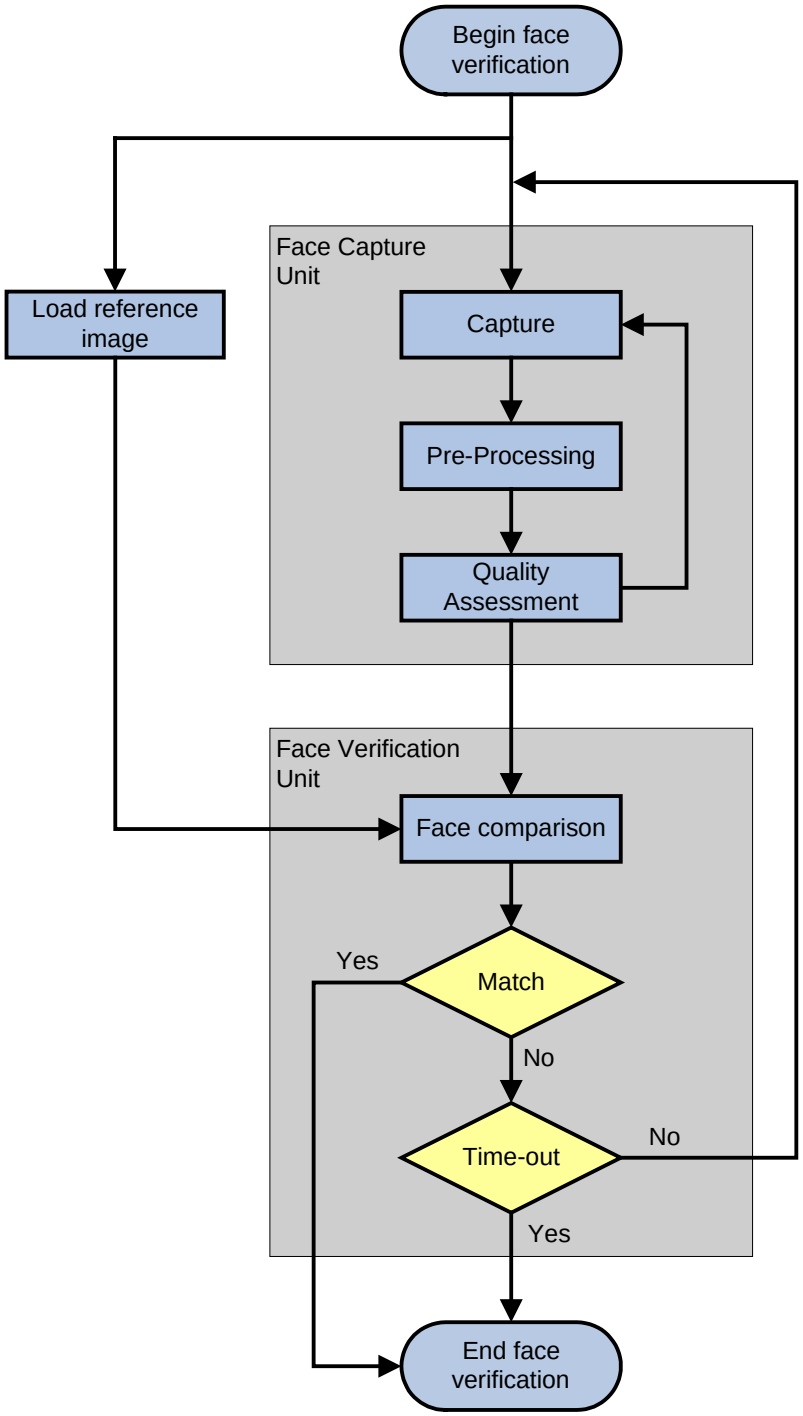


Figure 6: Face capture and verification process

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 [ISO19794-4], 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 [ISO19794-4], 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 re-calibration in the field or at least a necessary re-calibration MAY be possible for qualified service staff. It is RECOMMENDED that the compliance of a 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 lights. 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 cases, the chosen sensors should be able to operate under other (usually rougher) environmental constraints.

The unit SHALL be mounted in a way that users are easily able to position themselves in order to place their hands and thumbs on it. 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 in close neighbourhood to the sensor.
- Illuminated pictograms.
- LED's assigned to pictograms directly on the sensor.

The following information SHOULD be given to the user:

- Assistance to finger positioning with images and/or video on the screen and/or audio instructions (e.g. to instruct the user to move its fingers to the left/right/top/bottom).
- Visual and/or audio notification when a successful acquisition has been completed.
- 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 standard state of the art interfaces (e.g. USB2.0) SHALL be used.

It is RECOMMENDED to use standard interfaces according to BioAPI [ISO19784-1] 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 to the fingerprint verification unit.

The term "pre-processing", which is henceforth used, 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, e.g. minimum minutia count. The process of capturing SHOULD prefer the highest quality image of a sequence, at least the last captured image (after time-out) 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 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 following requirements SHALL be fulfilled:

- The fingerprint capture unit should have the ability to accept rotated fingerprints having the same direction in 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 [ISO19794-4]. 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 in [ISO19794-4], 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 used WSQ algorithm SHOULD be certified by the FBI and SHOULD be referenced by the respective certificate number (coded in the WSQ header).

Multiple glossy 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 one second per frame.

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

5.2.2. Fingerprint Verification Unit

5.2.2.1. 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 [ISO19784-1] 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.

5.2.2.2. 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 data format WSQ. 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 one 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 FTC (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.

Note: It is RECOMMENDED to perform the FAR calculation of the ABC system as an independent but parallel process as follows:

- The reference fingerprint images (DG3 images) of the last ten 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 to the applicable data protection regulations.
- The FAR is calculated on the basis of impostor comparison scores. Genuine comparison scores MAY be used to calculate the corresponding FRR. Due attention should be devoted 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 RECOMMENDED 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. This 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 draw off 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.

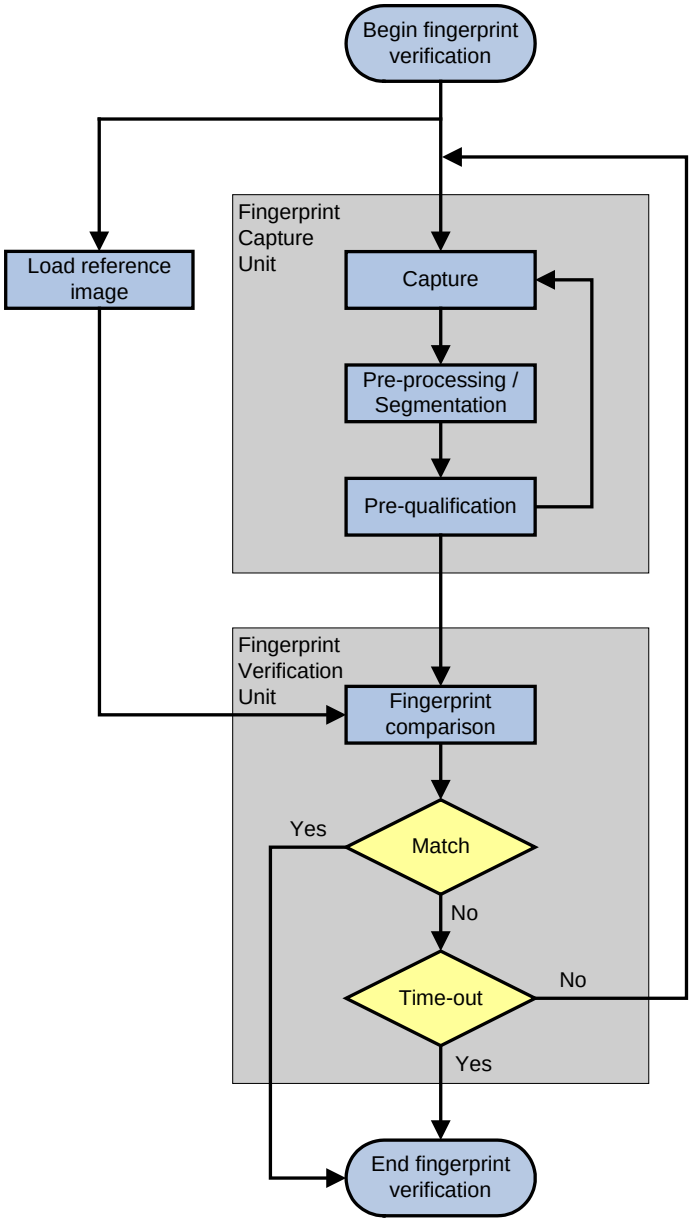


Figure 7: Fingerprint capture and verification process

5.3. Multibiometrics

The general schema for biometric system decision presented in Figure 8 is directly relevant systems to define the process of biometric verification in ABC (in this case, “Data storage” is provided by e-MRTDs).

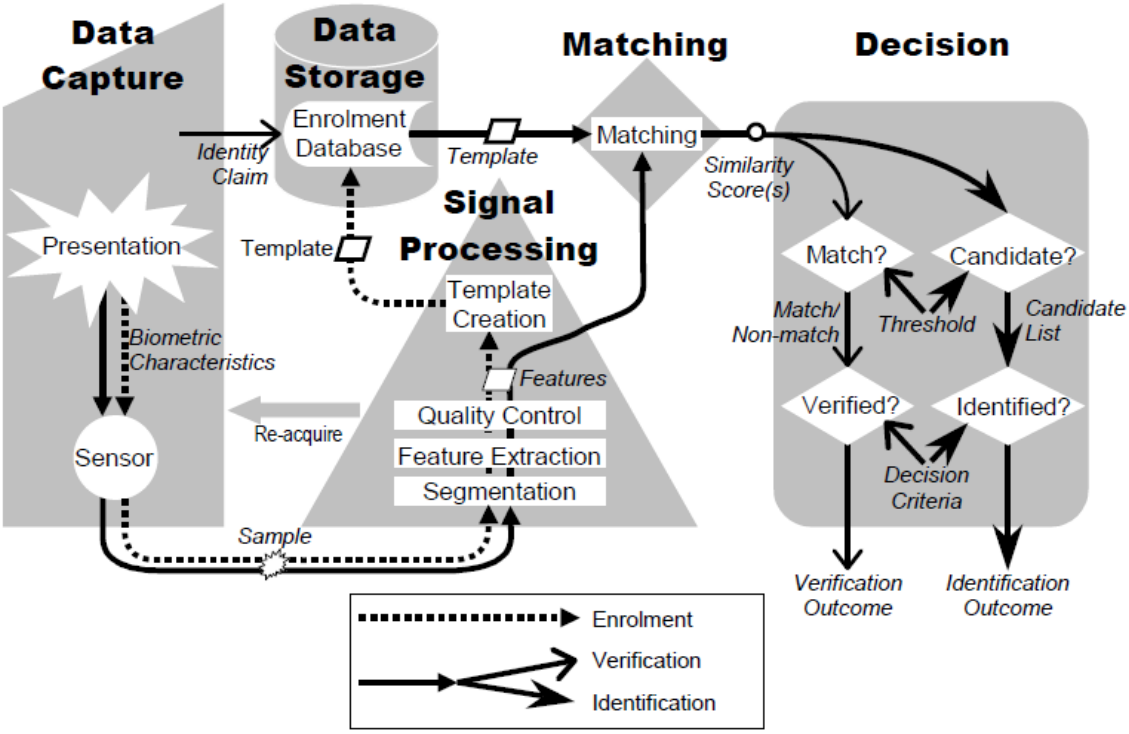


Figure 8: Schema for biometric system decision (from [ISO24741]). The reproduction of this figure has been authorised by ISO

Multibiometric 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, multibiometrics 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 multibiometrics MAY be incorporated in national implementations of ABC systems.

Descriptions about multibiometrics are presented in [ISO24722]. Several types of multibiometrics can be applied directly to ABC systems in order to improve 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.

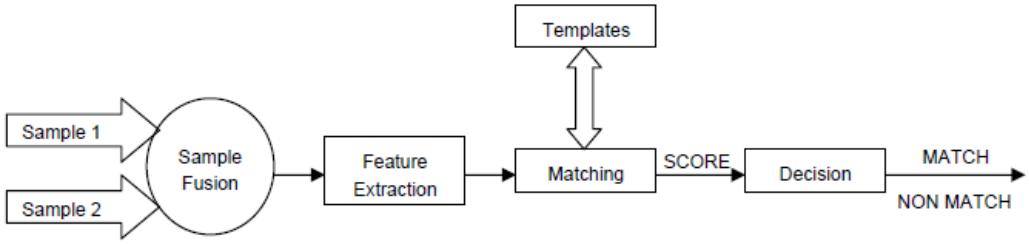


Figure 9: Sample level fusion in multibiometric systems (from [ISO24722]). The reproduction of this figure has been authorised by ISO

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.

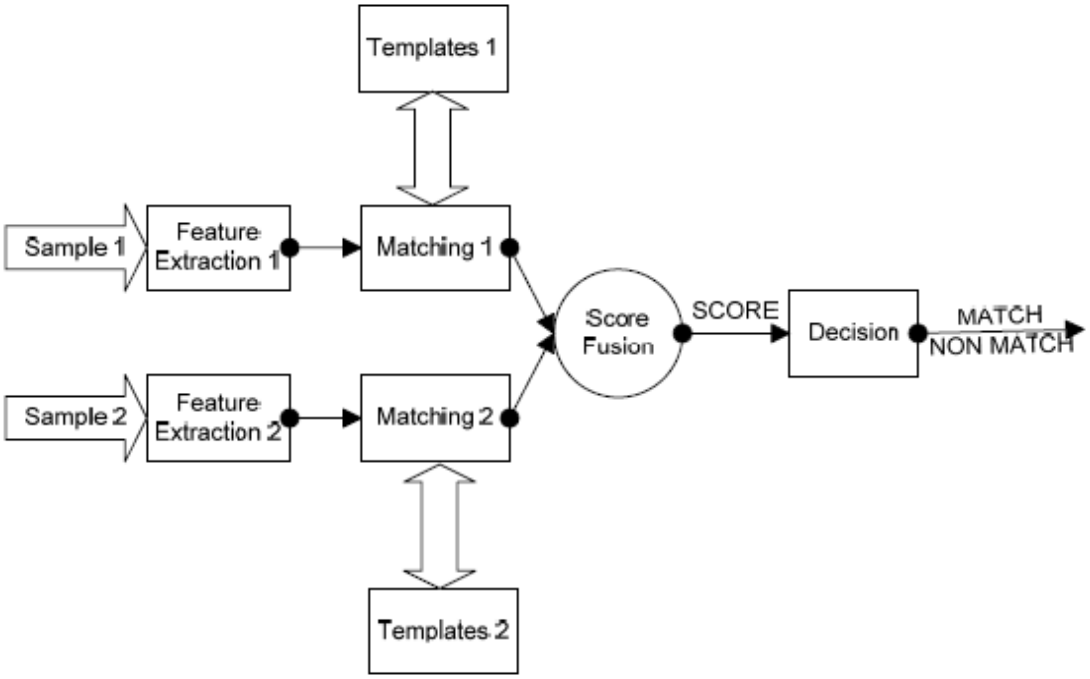


Figure 10: Score level fusion in multibiometric systems (from [ISO24722]). The reproduction of this figure has been authorised by ISO

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 on the process level that is able to process the input from several verification units.

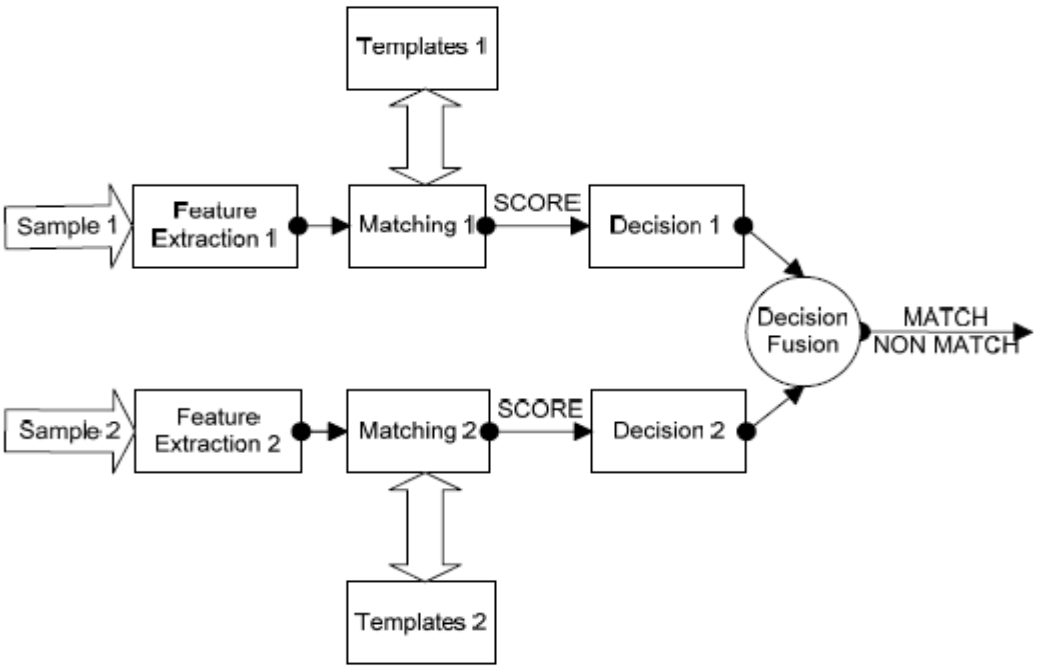


Figure 11: Decision level fusion in multibiometric systems (from [ISO24722]). The reproduction of this figure has been authorised by ISO

6. QUALITY CONTROL

Quality control is the process whereby the quality of all factors involved in the operation and exploitation of the ABC system are measured. Quality 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 quality control and the extraction of business statistics in ABC systems.

While quality control 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 for data storage for quality control 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 quality control 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.[10] Therefore

[10] *See in particular 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.*

personal data SHALL NOT be stored for the purposes of quality control and statistics extraction unless properly anonymized.

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

It is RECOMMENDED that 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 it is out of the scope of the basic functionality of an ABC system to provide built-in statistical analysis.

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

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

It is RECOMMENDED that each entry within the operational register is as complete as possible, depending on how far the verification process could be completed. 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 detail concerning the sorts of data which are of interest when logging for quality control 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 required 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 be 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 following timing information 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 its first interaction with the system (presentation of the travel document in an integrated two-step process ABC system, entry in the mantrap space in 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 shows:

- Module type (e.g. verification, access, monitoring, level 2).
- 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 a 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. 1st or 2nd generation e-Passport).

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

- Time period dedicated to the document authentication process as a whole (from the beginning of the 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 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 a 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.
- Time effort for the biometric verification process (from the beginning of the image capture until the provision of the final verification result).
- Delays resulting from the travellers' behaviour (time effort from the start of the capture process until the first successfully captured image is provided to the verification unit).
- Amount of single verification events within the verification process.
- At least the best comparison score of all single verification events within the face capture and verification process.
- 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 (from the beginning of the live sample capturing until the provision of the final verification result).
- Delays resulting from the travellers' behaviour (time effort from starting the capture process until the first successfully live sample is provided to the verification unit).
- Overall result of the verification process or, alternatively, the verification score and comparison threshold.
- Quality indicator of the best live sample (e.g. number of minutiae in a fingerprint).
- Quality indicator of the reference image, if available (e.g. number of minutiae in 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 this background checks are performed by accessing systems external to the ABC (such as a query to a Lost & Stolen Document Database). For this 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 following data 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. number of minutiae captured 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 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. number of minutiae captured 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

Boeing: *Current Market Outlook 2012-2031 – Long Term Market*, 2012.

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 October 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 February 2008.

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 on 3 August 2012].

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 on 20 August 2012].

Federal Office for Information Security: *Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, 27 November 2009* [PP0062].

Federal Office for Information Security: *Fingerprint Spoof Detection Protection Profile (FSDPP), Version 1.8, 23 November 2009* [PP0063].

Federal Office for Information Security: *Technical Guideline TR-03110 – Advanced Security Mechanisms for Machine Readable Travel Documents*, Parts 1, 2, and 3, 20 March 2012, Version 2.10, 20 March 2012 [BSI03110].

Federal Office for Information Security: *Technical Guideline TR-03121 – Biometrics for Public Sector Applications, Version 2.3, 2011* [BSI03121].

Federal Office for Information Security: *Technical Guideline TR-03129 – PKIs for Machine Readable Travel Documents*, Version 1.10, 9 November 2011 [BSI03129].

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

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 2.0.

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 on 3 August 2012].

ISO/IEC 14443: *Identification cards – Contactless integrated circuit cards – Proximity cards,* Parts 1-4 [ISO14443].

ISO/IEC 19784-1:2006, *Information technology – Biometric application programming interface,* Part 1: BioAPI specification [ISO19784-1].

ISO/IEC 19794-2:2011, *Information technology – Biometric data interchange formats,* Part 2: Finger minutia data [ISO19794-2].

ISO/IEC 19794-4:2011, *Information technology – Biometric data interchange formats,* Part 4: Finger image data [ISO19794-4].

ISO/IEC 19794-5:2011, *Information technology – Biometric data interchange formats,* Part 5: Face image data [ISO19794-5].

ISO/IEC 7816-11:2004, *Identification cards - Integrated circuit cards,* Part 11: Personal verification through biometric methods [ISO7816-11].

ISO/IEC TR 24722:2007, *Information technology – Biometrics – Multimodal and other multibiometric fusion* [ISO24722].

ISO/IEC TR 24741:2007, *Information technology – Biometrics Tutorial* [ISO24741].

Oxford University Press: *Oxford Dictionaries* [last accessed on 3 August 2012].

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

ANNEX 2: ADDITIONAL READING

Biometrics

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

Software Architecture	An example for detailed requirements on the software architecture can be found in [BSI03121-1] and [BSI03121-2].
Process of Biometric Verification	An example for detailed requirements on the process of biometric verification based on live captured face images can be found in [BSI03121-2], section "Verification ePassport and Identity Card using facial biometrics" and [BSI03121-3], section "P-PH-VID".
Face Capture Unit	An example for 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 for detailed requirements on the operational issues and can be found in [BSI03121-3], section "O-PH-VID".
User Interface	An example for 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 for a detailed logging scheme can be found in [BSI03121-3], sections "COD-PH-VID", and "LOG-PH-VID".

Certification of document readers

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

In order to verify the compliance of an eMRTD authentication sub-systems (e.g. electronic document reader hard- and software) to the relevant ISO and ICAO standards (especially [ISO14443], [ISO7816] and [ICAO9303]) it is common to rely on established evaluation and

certification schemes. Examples for 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 [BSI03105-4]

- 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 EAC 1.11 [BSI03105-51]

ANNEX 3: OPERATIONAL AND PLANNED ABC SYSTEMS IN THE EU/SCHENGEN AREA

OPERATIONAL

MS	SYSTEM DESCRIPTION	
DE	**System**	**EasyPASS**
	Go-live date	Started in August 2009 as pilot and since April 2010 has been operating as regular programme
	Eligible travellers	EU/EEA/CH citizens who are over18 and who old an e-Passport or a German e-ID card
	Location	Terminal 1 of Frankfurt/ Main Airport; installation of four e-Gates and one monitoring and control station
	Biometrics	Face
	Configuration	Integrated two-step solution with two e-Gates
	System owner	The system is owned by the German Federal Police
	System operator	The system is operated by the German Federal Police
	System supplier	L-1 identity solutions and Magnetic Autocontrol are the system providers. The integrator of EasyPASS is Secunet Security Networks AG. The e-Gate including the face capture unit is provided by L-1 Identity Solutions AG and Magnetic Autocontrol GmbH. The document reader and the belonging software for checking the optical security features are provided by Bundesdruckerei GmbH. There was a public tender for the installation and maintenance contract. The system is cleaned by the airport facility management employees and maintained by the Federal Police technicians and the contractor.
ES	**System**	**ABC system**
	Go-live date	It was established as a pilot project in May 2010 and an evaluation of the system was completed in January 2011. Since then it has been operating as a regular programme.
	Eligible travellers	EU/EEA/CH citizens who are over 18 and who old an e-Passport or a Spanish e-ID card
	Location	Madrid-Barajas, Terminals 1 and 4. Barcelona-El Prat, Terminals 1 and 2. An extension of the system to other Spanish airports is planned.

	Biometrics	Face and fingerprints
	Configuration	There are two different configurations in place: 1. Segregated two-step approach with one e-Gate in T1 MAD & T2 BCN 2. One-step solution based on a mantrap in T4 MAD & T1 BCN
	System owner	Sub-Directorate of Security Information and Communication Systems, Ministry of Interior.
	System operator	National Police
	System supplier	Indra is ther primary contractor and integrator of the back-end solution of the ABC system. The e-Gates have been supplied by Gunnebo. Facial and fingerprint recognition technology is provided by Neurotechnology.
FI	**System**	**ABC lines**
	Go-live date	A trial at Helsinki-Vantaa Airport was launched on 8 July 2008. After a successful evaluation, the system went operational in 2009. The ABC system has also been in operation at Vaalimaa land BCP (at the border with Russia) since 9 December 2009.
	Eligible travellers	EU/EEA/CH citizens who hold an e-Passport.
	Location	The system is available at Helsinki-Vantaa Airport and Vaalimaa land BCP. There are now ten e-Gates at the airport for departing passengers in non-Shengen Terminal. Ten additional e-Gates are available for arriving travellers at the exit/transfer side in Terminal 2. Five e-Gates are located at Vaalimaa BCP.
	Biometrics	Face.
	Configuration	Two-step process with two e-Gates. At arrivals there are upgraded Vision-Box e-Gates where the standing mat is removed and the e-Passport reader is positioned directly in front of the traveller, which is considered more user-friendly. Changes for departing side e-Gates were introduced during autumn 2011. e-Gates are automated with supervision. There is one operator per five to ten e-Gates, depending on the volume of traveller flows.
	System owner	The system is owned by the Finnish Border Guard.
	System operator	The system is operated by the Finnish Border Guard.
	System supplier	The technology and maintenance provider is Vision-Box.

FR	**System**	**PARAFE**
	Go-live date	The project launched in 2007 and the system has been operational since December 2009.
	Eligible travellers	EU/EEA/CH citizens over 18 years old as well as Third Country Nationals who are family members of EU citizens. In order to use the system, travellers must hold an e-Passport and register in a specific police database. There are plans to support also French IDs.
	Location	The system is available at Orly and Paris-Charles-de-Gaulle Airports
	Biometrics	Fingerprints.
	Configuration	One-step process, mantrap solution.
	System owner	The system owner is the Border Police.
	System operator	The system operator is the Border Police.
	System supplier	The technology is provided by Morpho.
NL	**System**	**No-Q**
	Go-live date	The system went live on 27 March 2012.
	Eligible travellers	EU/EEA/CH citizens who are holders of an e-Passport. Minors (i.e. persons under18) are not allowed although they can go through the process and will then be referred to manual controls.
	Location	The system is available at Schipol International Airport – initially at arrivals (from the kick-off date) and at then also at departures. There are plans to install the system at transfers later on.
	Biometrics	Face
	Configuration	One-step solution
	System owner	Accenture owns the hardware and the ABC server. The Ministry of Interior owns the No-Q server, which decides on the input that is given by the ABC server, and the connections to other (background) databases.
	System operator	The system operator is the Dutch Royal Marechaussee

	Technology supplier	Accenture is the main integrator and the software developer. The hardware is supplied by Vision-Box.
NO	**System**	**ePassport Gates**
	Go-live date	The system went live in June 2012.
	Eligible travellers	
	Location	Arrivals at Oslo Gardermoen Airport (OSL). It is planed to extend it to the land border with Russia during the third or fourth quarter of 2012.
	Biometrics	Face.
	Configuration	Integrated two-step process with mantrap. The e-Passport is read before the traveller enters the mantrap and a facial image is captured once inside.
	System owner	The system is owned by the Norwegian Police Border Guard.
	System operator	The system is operated by the Norwegian Police Border Guard.
	Technology supplier	System integrator/technology provider: Gemalto/Vision-Box
PT	**System**	RAPID
	Go-live date	The system started operating in 2007, first as a pilot and then as a permanent programme.
	Eligible travellers	EU/EEA/CH citizens over 18 years old who are holders of an e-Passport.
	Location	All international airports. Seaports installations have been discontinued
	Biometrics	Face
	Configuration	Integrated two-step solution with a double e-Gate
	System owner	The system owner is the Immigration and Border Service (SEF).
	System operator	The system is operated by the Immigration and Border Service (SEF).

	Technology supplier	Vision-Box
UK	**System**	**ePassport Gates**
	Go-live date	The system went live in 2008.
	Eligible travellers	EU/EEA/CH citizens over 18 years old who are holders of an e-Passport.
	Location	The system is available at arrivals in the following airports: Bristol, Birmingham Terminals 1 and 2, Cardiff, East Midlands, Gatwick North, Gatwick South, Heathrow at all 4 terminals, Manchester Terminals 1 and 2. The total number of e-Gates which have been installed amounts to 15.
	Biometrics	Face
	Configuration	There are different configurations in place: 1. Double e-Gate (Manchester, Vision-Box) 2. Single e-Gate (Stansted, Accenture) 3. Virtual Second Entry Gate (Accenture, Heathrow) There is one UKBA operator and one referral officer for every three e-Gates.
	System owner	The system owner is the UK Border Agency (UKBA).
	System operator	The system is operated by the UKBA.
	Technology supplier	Fujitsu in partnership with Visionbox or Accenture depending on site.

PLANNED

MS	DESCRIPTION	
AT	**State of play**	Pilot phase
	Planned go-live	Pilot phase planned October 2012 until August 2013
	Location	Vienna International Airport , 1 Pilot System
	Biometrics	Face
	Configuration	Integrated two-step solution
	System owner	Since it is a Pilot Project, the system is owned by the technology supplier.
	System operator	The system is operated by the Austrian Federal Police in close cooperation with the project partners which are Vienna International Airport, Austrian Institute of

		Technology (AIT), and the technology supplier.
	Technology supplier	Gunnebo, ATOS
BE	**State of play**	Project launched on June 2011
	Planned go-live	2012
	Location	Brussels National Airport
	Biometrics	N/A
	Further information	Border management authority is working in close cooperation with the airport operator.
CZ	**State of play**	EasyGo system. In a pilot phase.
	Planned go-live	The installation was completed on 21 November 2011.
	Location	Prague-Ruzyne Airport (only one e-Gate initially)
	Biometrics	Face
	Further information	The configuration chosen is the one in use at Frankfurt (EasyPASS)
DK	**State of play**	Project launched in October 2011. Currently in the research phase
	Planned go-live	Go-live will take place in 2013 at the earliest
	Location	N/A
	Biometrics	N/A
	Further information	N/A
EE	**State of play**	The project was launched in January 2011 and the procurement process will start in 2012.
	Planned go-live	2012
	Location	Tallinn Airport (two e-Gates at entry and two at exit, accompanied by three kiosks each).
	Biometrics	Face and fingerprints
	Further information	The target group are EU/EEA/CH citizens over15 years old who hold an e-Passport
HU	**State of play**	Currently in the planning phase
	Planned go-live	2013

	Location	Budapest international Airport
	Biometrics	Fingerprints
	Further information	The target group are EU citizens holding e-Passport, registered travellers and members of the crew of the National Airline Company.
LV	**State of play**	Pilot planned.
	Planned go-live	Mid-2014.
	Location	Riga International Airport (two e-Gates at the transit zone)
	Biometrics	Face
	Further information	The aim is to shorten connection times within a context of scarce resources. Provisionally a mantrap configuration has been chosen. The target group are EU citizens holding an e-Passport. The e-Gates should be switchable between entry and exit.
RO	**State of play**	Pre-acquisition phase.
	Planned go-live	End of 2011/first trimester of 2012.
	Location	International Airport Henri Coanda, Bucharest (1 e-Gate at entry and another at exit)
	Biometrics	N/A
	Further information	It will probably be configured as a mantrap. The "National Printing Office Company" will own the system, although its use will be transferred to the Romanian Border Police. The Romanian Border Police operate the system, in cooperation with the airport operator.

TT-30-12-751-EN-N

ISBN 978-92-95033-58-0

doi:10.2819/26969

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

www.frontex.europa.eu
Rondo ONZ 1, 00-124 Warsaw, Poland
Tel. +48 22 205 95 00
Fax +48 22 205 95 01