FRONTEX

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

FRONTEX

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

Research and Development Unit

FRONTEX

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

Research and Development Unit
Capacity Building Division

Plac Europejski 6
00-844 Warsaw, Poland

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

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

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

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

Date: September 2015

Contents

Legal notice #6

All rights reserved #6

Acknowledgements #7

About Frontex #8

Acronyms and abbreviations #9

Glossary #10

Executive summary #16

Terminology #20

1. Introduction #21
   - 1.1. Purpose and audience #21
   - 1.2. Scope and methodology #21
   - 1.3. About best practices and guidelines #23
   - 1.4. How to read this document #24

2. General overview of ABC systems #25
   - 2.1. Concept #25
   - 2.2. Main functions and features #25
   - 2.3. Advantages of automation #26

3. Operational considerations for automated border control #28
   - 3.1. Overview of the Border Checks Process #28
   - 3.2. General process flow #28
   - 3.3. Operational requirements #29
   - 3.4. Functional requirements #30
     - 3.4.1. Checking the document authenticity/validity #30
     - 3.4.2. Identity verification #32
   - 3.5. Implementation of ABC system #32
     - 3.5.1. Decision-making process #32
     - 3.5.2. Equivalence of performance #39
     - 3.5.3. Cooperation with third parties #39
   - 3.6. Deployment of ABC system #40
     - 3.6.1. Topologies of ABC system #40
     - 3.6.2. Physical infrastructure: arrangement of the e-Gates and the monitoring and control station #42
     - 3.6.3. Environmental factors #42
     - 3.6.4. Integration in the host environment #43
     - 3.6.5. Flexibility to accommodate changes #43
   - 3.7. Personnel management and ABC systems #46
     - 3.7.1. Roles and tasks of personnel #46
     - 3.7.2. Training of personnel #49

3.8. Handling of exceptions #49
3.8.1. System malfunctioning #50
3.8.2. e-Gates out of service #50
3.8.3. Tailgating #50
3.8.4. Minors #50
3.8.5. Travellers with disabilities #50
3.8.6. Trespassing #51
3.8.7. Ineligible travellers #51
3.8.8. e-Passport is wrongly placed into the reader #52
3.8.9. Non-cooperative behaviour at the e-Gate #52
3.8.10. Anomalies in chips #52
3.8.11. Database hit #52
3.8.12. Failed biometric verification #52
3.8.13. Wrong or no security features on the biographical data page #52
3.9. Quality assurance and statistics #53

4. Traveller experience #54
4.1. Awareness and education before the e-Gate #54
4.1.1. Key messages to be transmitted #54
4.1.2. Delivery methods #55
4.1.3. Need for standard signs, instructions and logos #55
4.2. Running a traveller-friendly service at the e-Gate #56
4.2.1. Instructions at the e-Gate #56
4.2.2. Effectiveness of delivery methods #57
4.2.3. Managing traveller flow #58
4.2.4. Learning by observation #58
4.2.5. Traveller interaction with the e-Gates #59
4.2.6. Use of text and multiple languages #59
4.2.7. Human support at the e-Gate #60
4.3. User-friendly design of the e-Gate #60
4.3.1. System design #60
4.3.2. Attractiveness and safety #61
4.3.3. Ergonomics #61
4.4. Privacy and data protection #61

Annex 1: References #63

Annex 2: Overview of ABC systems in the EU/Schengen Area #66

Release Note and Table of Changes

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

Table of changes

Section Altered	Change
Acknowledgements	Names of experts, stakeholders and Frontex staff who contributed to the revision updated accordingly
About Frontex	Changes made to the title of this section as well as to the sentence about the core objective of the Capacity Building Division
Glossary	Updated according to the text, definitions added, introduction of some clarifications
Section 1.1.	Introduction of clarification regarding the purpose of the guidelines
Section 1.2. and 3.5.1.3.	Introduction of updates regarding the biometrics used
Section 1.3.	Introduction of clarification and updates regarding the definition of best practices
Section 2.1.	Introduction of clarifications regarding the definition of the ABC systems and updates regarding biometrics used
Section 2.2.	Introduction of updates regarding the Smart Borders Proposal and processing of third country nationals
Section 2.3.	Introduction of clarifications and updates regarding the audience of ABC systems in the EU
Section 3.2.	Introduction of clarifications regarding the diagram illustrating a border check process, introduction of changes in the terminology used in Figure 1
Section 3.3.	Introduction of changes regarding monitoring and operation of e-gates as well as risk assessment
Sections 3.4.1., 3.4.2.1. and 3.4.2.3.	Introduction of clarifications regarding determining travellers' eligibility, checking document validity and authenticity
Section 3.5.1.4.	Introduction of updates and clarifications regarding software and hardware procurement, in particular the interfaces between the system's components, obsolescence and creating one's own software
Sections 3.5.1. and 3.5.1.5.	Introduction of recommendations regarding vulnerability study/assessment
Section 3.5.1.6.	Introduction of recommendations regarding white-hat vulnerability and penetration testing
Section 3.5.2.	Introduction of recommendations regarding biometric performance testing and the assessment of ABC systems in operational environment
Section 3.6.1.	Introduction of clarifications regarding ABC systems topologies
Section 3.6.5.1.	Introduction of clarifications and updates regarding the assumptions of the usage of an e-Gate in the context of the optimal dimensioning of the system
Section 3.6.5.3.	Introduction of an update regarding the usage of wireless connections
Section 3.6.5.5.	Introduction of recommendations regarding maintenance
Section 3.6.5.6.	Introduction of a section on business continuity
Section 3.7.1.3.	Introduction of updates and clarification regarding the supervision of e-Gates by an operator
Section 3.7.2.	Introduction of a recommendation regarding the development of common EU training
Section 3.8.5.	Section expanded to include recommendations of the European Disability Forum
Section 3.8.7.	Introduction of clarifications regarding the ineligible travellers
Section 3.8.12.	Introduction of updates regarding recommended procedure in case of failed biometric verification
Section 3.9.	Harmonisation of terminology regarding quality assurance
Section 4.1.3.	Recommended logo for ABC system updated
Section 4.2.1.	Introduction of updates regarding the use of audio and visual instructions
Section 4.2.6.	Introduction of updates regarding the use of multiple languages in ABC systems
Section 4.4.	Section expanded to include the information on the proposed Data Protection Regulation, applicable provisions of international law and the European Data Protection Supervisor's recommendations on 'Privacy by Design'
Annex 1	References updated according to the text
Annex 2	Introduction of updates regarding operational and planned ABC systems in the EU

Legal notice

All rights reserved

Before citing the Frontex Best Practice Operational Guidelines for Automated Border Control (ABC) Systems:

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

In the introductory part of the document:

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

In the body of the document:

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

In the references section:

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

Frontex RDU contact data:

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

Acknowledgements[1]

This report was prepared by the Research and Development Unit (RDU) of Frontex in close collaboration with experts from a number of EU Member States which, at the time of writing, were operating or testing an ABC system at a number of border crossing points of the European Union and other stakeholders who have commented and provided contribution to the drafting and revision of the present report. Frontex would like to particularly acknowledge the work of the following persons who participated in the Working Group on Automated Border Controls:

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

In addition Frontex is grateful to Ciaran Carolan (eu-LISA, the EU Agency for the operational management of large-scale IT systems), Kerry Kwan (Immigration Department of the Hong Kong Administrative Region), and Ted Dunstone (Biometrics Institute and Biometix) who have extensively contributed to the revision of the present document. Furthermore, Frontex appreciates the comments sent by European Civil Aviation Conference (ECAC), and European Disability Forum (EDF). Frontex have also taken on board the remarks reflected in FRA (Fundamental Rights Agency) Annual Activity Reports[2] during the revision process.

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

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

[2] **FRA Annual Activity Report 2012** *http://fra.europa.eu/sites/default/files/annual-report-2012_en.pdf*
FRA Annual Activity Report 2013 *http://fra.europa.eu/sites/default/files/fra-2014-annual-report-2013_en.pdf*

About Frontex

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

The core objective of the Capacity Building Division is to drive the process of harmonisation and standardisation for border control and 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's main areas of work is the exploration of the potential offered by new border management technologies to meet the dual objective of enhancing security while facilitating travel.

Acronyms and abbreviations

ABC	Automated Border Control
BAC	Basic Access Control
BCP	Border Crossing Point
BPGs	Best Practice Guidelines
BPOGs	Best Practice Operational Guidelines
BPTGs	Best Practice Technical Guidelines
CBA	Cost Benefit Analysis
CCTV	Closed Circuit Television
e-MRTD	Electronic Machine Readable Travel Document
EC	European Commission
ECtHR	European Court of Human Rights
EJEU	Court of Justice of the European Union
EU	European Union
EU/EEA/CH	European Union/European Economic Area/Switzerland
FAR	False accept rate
FoM	Figure of Merit
FRR	False reject rate
ICAO	International Civil Aviation Organisation
ISO	International Organisation for Standardisation
IT	Information Technology
ITIL	Information Technology Infrastructure Library
MMI	Man Machine Interface
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
MS	EU Member State
NL	Netherlands
PKD	Public Key Directory
PKI	Public Key Infrastructure
RF	Radio Frequency
RTP	Registered Traveller Programme
SBC	Schengen Borders Code
SLA	Service Level Agreement
TCN	Third Country Nationals
UK	United Kingdom
UV	Ultra Violet
VIZ	Visual Inspection Zone
WG	Working Group

Glossary[3]

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 cooperation with the operator of the e-Gates.

Authentication process: A process that validates the claimed identity of a participant in an electronic transaction.

Automated Border Control (ABC) system: An automated system which authenticates the electronic machine readable travel document or token, establishes that the passenger is the rightful holder of the document or token, queries border control records, then determines eligibility of border crossing according to the pre-defined rules.

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

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

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

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

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

Border Guard: Any public official assigned, in accordance with national law, to a border crossing point or along the border or the immediate vicinity of that border who carries

[3] The definitions included in this section are based on a number of relevant glossaries and dictionaries, namely the European Migration Network Glossary, the ICAO MRTD Glossary, ISO Information Technology 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.

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 with the introduction of new border control technologies. The aim is to promote the development among the staff of new attitudes and behaviour that are instrumental to the introduction of the new processes required for the operation of those technologies (i.e. the ABC system).

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

Customer Service Personnel: Within the context of 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'.*

EasyPASS: Automated Border Control System in Germany.

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

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

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

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 the State's internal specifications or the bilateral agreed specifications between States sharing this information. See also 'Basic Access Control (BAC)'.

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

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

First-Line Check: Default checks carried out at border crossing points to ensure that travellers are authorised to enter or exit the territory of the Member State. 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*'.

Identification: The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the e-Passport holder whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with 'verification'.

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 pass as another person for the purpose of using that person's document or a person who unintentionally passes as someone else. See also '*zero effort impostor attempt*'.

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 comparison and other applicable checks are carried out. This topology is invariably implemented by using a mantrap e-Gate. See also '*One Step Process*' and '*Segregated Two-Step Process*'.

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

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

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

Member State: A country which is a 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 to 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)*'.

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 '*Registered Traveller Programme*'.

Schengen Area: An area without internal border control encompassing 26 European countries, including all EU Member States except Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom, as well as four non-EU countries, namely Iceland, Lichtenstein, Norway and Switzerland. 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 separate. 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*'.

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.

Spoofing: A tactic to exploit a biometric vulnerability caused by the manufacture of a disguise, prosthetic or other obscuration designed to either avoid detection or to be incorrectly identified as another person.

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 Community 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 and/or arranged.

Verification process: The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. Contrast with '*Identification*'.

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)'*.

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

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

Zero Effort Impostor Attempt: An impostor attempt is classed as 'zero-effort' if an *individ*ual submits his or her own biometric characteristics as if he or she were attempting successful verification against someone else's template. See also *'Impostor'*.

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 operational dimension.

These Best Practice Guidelines (BPGs) have been drafted by the Frontex Working Group (WG) on ABC in an effort to promote harmonisation of practice, similar traveller experience and minimum required security levels at the different BCPs where ABC systems have been deployed. The **intended audiences** are decision-makers, project managers and practitioners involved in the design, implementation and operation of ABC systems in the EU Member States (MSs). While these ABC Best Practice Operational Guidelines (BPOGs) have been conceived as a stand-alone resource, ideally they should be read in combination with the Frontex 'Best Practice Technical Guidelines for ABC Systems (BPTGs)'. Additional documents such as Guidelines for Processing third country nationals through ABC and ABC Challenge Catalogue (forthcoming) should serve as the complementary documents to these BPGs.

The document focuses on ABC systems based on the use of an electronic travel document (generally an ICAO-compliant e-Passport) which can be used by EU citizens without the need of pre-enrolment. Registered Traveller Programmes (RTPs) are outside its scope[4]. The **biometric markers** covered include both facial recognition and fingerprints.

The BPOGs are structured in **two main areas**. The first proposes guidelines and recommendations on the **operational dimension of ABC**, such as its operational and functional requirements, the implementation process, the system possible topologies and its integration in the host environment, the roles and tasks of personnel, the handling of exceptions and business continuity. The second addresses issues related to the **traveller experience**, including methods for awareness-raising among travellers, to deliver usage instructions and to achieve a high-quality and user-friendly service.

The Schengen Borders Code (SBC), the EU Visa Code and national legislation set the framework for the various measures which are implemented at the BCPs of the Schengen Area. Yet the detailed operational model followed at each BCP is designed to target the specific situational requirements, which often leads to differences among the various implementations.

Border checks are the checks conducted at BCPs to ensure that a person, including their means of transport and the objects in their possession, may be authorised to enter the territory of the MSs or authorised to leave it. In the traditional, manual border control process, such checks are carried out by border guards. In contrast, when an ABC system is in use, some of the steps in the process are automated whereas others are carried out by the traveller as self-service. The overall traveller processing time of an e-Gate should be comparable to or faster than that of a manual line. However, in general the outcome (i.e. acceptance/rejection) should be the same, irrespective of whether checks are automated or manual. Further-

[4] For a more detailed information as regards processing third country nationals through ABC, please refer to Frontex Guidelines for Processing third country nationals through ABC.

more, in order to achieve basic operational harmonisation across EU implementations, some **general operational requirements** must be observed by any ABC implementation, for example in relation to the monitoring process and the handling of exceptions.

There are also some basic **functional requirements** which should be respected. ABC systems must be able to confirm whether a travel document is genuine by examining its optical and electronic security features, and to verify the identity of the traveller by comparing the biometric data stored in the e-Passport chip with a biometric sample captured live from the traveller. In addition, the biographic data of the traveller may be checked against available databases.

The **implementation of an ABC system** is a complex process involving the mobilisation of significant economic resources and requiring the cooperation of a number of stakeholders. A phased decision-making approach can help the responsible authorities stay away from previously known risks and avoid costly mistakes.

The development of a sound **Business Case**, which clearly identifies the key objectives of the implementation, should be the starting point for any ABC deployment. An honest **Cost Benefit Analysis (CBA)** is the most critical part of the business planning process. If properly executed, the CBA should provide a valuable insight into the cost and benefits associated with the deployment and operation of the ABC system in comparison with the baseline scenario, i.e. manual checks. It is advisable to follow a proven methodology that provides a structured, understandable, efficient, repeatable and low-risk approach. To foster harmonisation, Frontex has developed a complete framework comprising the tools and data for the modelling, simulation and CBA of ABC systems and may be contacted before embarking on the CBA of an ABC system.

The **procurement process** can also play a critical role in the delivery of the ABC implementation strategic objectives. Different possibilities exist regarding what to tender: (1) to tender the product so that it will be the property of the tendering body, (2) to tender the product as a service. The latter means that the tendering body will not add property to their inventories but will enter into a service management contract with the supplier based on a Service Level Agreement (SLA), which has the advantage of accruing greater flexibility.

In order to fulfil the needs of the primary user, the authorities should define a set of requirements that create or reshape a product or components which can be acquired from the market. The tender terms of reference should also formulate knock-out criteria specifying technical and functional requirements with which the supplier has to comply in order not to be excluded from the tendering process. All offers need to be ranked on the basis of the tender criteria according to the offered prices, with a lower limit in place to avoid 'dumping' practices.

Any large-scale installation should be preceded by a **pilot** to identify key issues and reduce the risks of the final deployment. A research or benchmarking phase can help the authorities decide upon the system(s) which should be implemented in the pilot stage. This would involve testing and comparing a number of systems and designs available in the market across several dimensions, the most important of which are the system's overall stability, security and service management. A pilot would then enable MSs to further evaluate the design and performance of the chosen system, including its Man Machine Interface, and to make changes before committing to a large-scale deployment.

Besides the border management authority, **other key actors** who need to be effectively engaged in the implementation process are the port operator, the relevant carriers and the supplier of the ABC technology. The **port operator**, in particular, can critically impact on the levels of usage of the e-Gates by influencing the location of the ABC system and facilitating awareness raising among travellers. Port operators may also contribute to the installation of an ABC system by providing financial support as long as they also accrue benefits from the system.

Suppliers, on the other hand, are responsible for ensuring support to the operation of the system. SLAs should be clearly defined, including response times and penalties where applicable, in order to guarantee that cooperation with the suppliers is maintained at satisfactory levels.

In general there are three **topologies** of ABC systems 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 eligibility to use the system at the first stage and then, if successful, move to a second stage where a biometric comparison and other applicable checks are carried out. Finally, in the '**segregated two-step process topology'** the verification processes and the crossing of the actual border take place at separate locations.

As regards the **physical infrastructure** for the ABC system, synergies can be achieved by placing the manual and the automated lines (EU/EEA/CH) next to each other. The monitoring and control station for the e-Gates may be built in a way so as to allow manual first line checks in the case of an ABC system being out of service due to system crash, repair or maintenance. Having a fall-back solution in place for the event of a system failure is particularly relevant in the early stages of an installation or if the design is untested.

There is an inherent trade-off between service excellence and cost-effectiveness that needs to be carefully balanced. For any given amount of traveller flow, more e-Gates will reduce queuing time but at the same time will use more resources (financial, material and human). A recommended way to determine the optimum number of e-Gates for a new installation or to decide on the upgrading of an existing one is by means of operational research. In particular, queuing analysis would show the relationship between the three key variables: flow rate, service quality and lifecycle cost.

'Cold lines' (i.e. stand-alone unsupervised e-Gates) must not occur, as they would not guarantee acceptable levels of facilitation and security. Border guards may be assigned two **main roles** in the operation of an ABC system: operator and/or assisting personnel. The **operator** is responsible for the remote monitoring and control of the ABC system and its users. A single border guard can typically supervise from three to 10 e-Gates, although the average number in MSs with operational ABC systems currently sits at five. **Assisting personnel** (not to be confused with customer service staff) work closely with the operator, handling exceptions that take place at the e-Gates, redirecting travellers as needed and assisting them on specific situations.

Acceptance of the ABC system by border guards is crucial for its successful operation. Pro-active **change management** to engage staff and address their concerns has proven successful in reducing resistance to the introduction of the ABC implementation. In addition, initial and follow-up **training** will be required so that officers can operate the system successfully and contribute to its enhancements. A select number of officers may be trained as expert users to act as a first line of defence when technical issues occur.

Border guards need detailed instructions on how to deal with specific **exceptional situations**, including system malfunctioning, non-cooperative behaviour at the e-Gate, anomalies in e-Passport chips, etc. These could be usefully specified in a modus operandi handbook (e.g. ABC Handbook for Border Guards).

Quality assurance is a process by which the quality of all factors involved in the operation and exploitation of the ABC system are measured. The retrieval from the system of a certain amount of anonymous operational data is required for the purposes of quality control and for the extraction of business statistics. ABC systems are subject to the same **privacy and data protection requirements and legislation** as applicable to any other system entailing the processing of personal data. The storage without proper justification of personal data identifying the traveller should be avoided.

Only if a significant number of travellers use the system will the investment made be justified. Thus, achieving a satisfactory **traveller experience** is key for the success of an implementation. While ABC systems currently provide a similar service to travellers, there are a number of differences between implementations, not only in appearance, but also in functionality and usage. This lack of universality, together with the relative novelty of such systems, makes the task of harmonising the expectations and usability a difficult one.

Making the traveller aware that an ABC system is available at a particular port is critical to getting more travellers to leave the queue for the manual control. Travellers should be helped to understand the benefits that the system brings to users, informed that they are eligible if this is the case and instructed on how to use the e-Gate. Information can be delivered through a variety of methods, including signs and logos, videos, leaflets and human assistance.

Signs, in particular, are very important as they often represent the first contact that the traveller has with the system. One of the key challenges lies in developing a set of signs and standard terminology across different national implementations that can be understood by the majority of the travellers. In the absence of a common name, the term '**Self-Service Passport Control**' may be used in order to denote the existence of an ABC system.

Providing clear **instructions** at the e-Gate is essential in order to run a user-friendly service. If possible, this should be combined with the provision of human assistance at the e-Gates through **customer service personnel.** This would generally consist of staff of the port operator which is tasked with providing guidance and advice to travellers in using the ABC system. Customer service personnel can also help manage the traveller flow by balancing it among the different e-Gates.

Ultimately, the ability of travellers to use the system easily and effectively will have a critical impact on its levels of usage and on the volume of rejections yielded. An implementation which is attractive and user friendly is thus crucial.

Terminology

Although the recommendations and guidelines presented in this document are non-binding for Member States, the present terminology has been adopted[5] 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 the European Union's external 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.

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

1. Introduction

1.1. Purpose and audience

The present report constitutes an update of the 'Best Practice Operational Guidelines for Automated Border Control' [last reviewed on 31.8.2012] and presents a compendium of best practice guidelines on the design, deployment and operation of automated border control (ABC) systems. These have been elaborated in an effort to achieve harmonisation of practice, similar traveller experience, and minimum required security levels at the different border crossing points (BCPs) of the European Union/Schengen Area where ABC systems have been or are to be deployed.

The intended audiences are decision-makers, project managers and practitioners involved in the design, implementation and operation of ABC systems in the EU Member States (MSs). Decision-makers both at the EU and national level will benefit from a better understanding of ABC systems, what they are, how they work and more importantly how these help to manage the unavoidable security, facilitation and cost trade-offs in border checks, thus allowing for better-informed decisions when it comes to allocating scarce human and financial resources.

The project managers from border management authorities will find detailed information in order to define its requirements and procure and implement a system that performs up to standards while staying away from previously known risks. Finally, current and prospective practitioners, i.e. border guards and port operator personnel, will benefit from a wealth of practical information on what to do, and also what to avoid, in order to run an ABC system in an effective, efficient and user-friendly way.

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

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[6].

Travel documents considered

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

[6] See in particular EC, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Preparing the next steps in border management in the European Union', COM(2008) 69 final, 13.2.2008; ICAO, 'Guidelines for electronic – Machine Readable Travel Documents & Passenger Facilitation', Version – 1.0, 17.4.2008.

e-Passports. This document focuses on ABC systems based on first- and second-generation e-Passports and also national e-ID cards[7]. There are no specific provisions in this document for combined or stand-alone use of ABC systems serving RTPs.

Biometric markers used

ABC systems currently in use support either facial or fingerprint recognition as the main biometric authentication method, with an exception for a few RTP systems supporting iris recognition. However, there is a large base of second-generation e-Passports carrying both facial and fingerprint data and there are some MSs which have gained relevant experience in the use of fingerprints for identity verification in ABC systems[8].

Methodology

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

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

The methodology used by the Working Group (WG) to develop the initial BPGs was based on the following tasks:

- state the problem and goals,
- elaborate the list of relevant topics to be covered,
- carry out research on current practice based on questionnaires, interviews and technical meetings,
- analyse results and extract individual best practices,
- debate and agree on proposed best practices,
- build the document,
- conduct an internal and external review of the document,
- approve these guidelines.

The WG decided to revise the 2012 release of the BPOGs to reflect new developments, including those regarding policy direction and the applicable legislative framework, and changes in MSs' practice. The main changes are summarised in the Table of Changes included in the beginning of this document.

[7] 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 two fingerprints in addition to the facial image.

[8] Fingerprint recognition is already implemented in several MSs' ABC systems. Additionally, the EC is also considering face, fingerprints and iris as the basis for an eventual EU RTP for third country nationals (TCNs). Thus, fingerprint recognition is covered in the present version of this document. For further details please refer to: PwC, 'Technical Study on Smart Borders; Final Report', October 2014.

During the revision process, information has been collected through regular expert discussions at the WG meetings, questionnaires[9], and field visits to MSs with ABC systems in operation as well as by gathering feedback from external stakeholders. The document has undergone extensive internal and external revision and the main modifications introduced have been debated and agreed during the expert WG meetings and teleconferences.

While there are limitations to the reliability of expert judgement in classifying certain practices as 'best'[10], it is understood that the BPGs outlined in this document are only recommendations which are **useful** and **effective –** they have proved their relevance to meet the needs and achieve the goals of the border management authority; they are potentially **transferrable** and **adaptable.**

1.3. About best practices and guidelines

The identification of best practices for automated border controls should be put into the context of conceptual and methodological issues pertaining to best practice research. While there is not a generally agreed understanding of what 'best practices' are, the Schengen Catalogue, which is used as a reference tool for Schengen evaluations, defines the term as 'a non-exhaustive set of working methods or model measures which must be considered as the optimal application of the Schengen *acquis*, on the understanding that more than one best practice is possible for each specific part of Schengen cooperation'[11]. For the sake of consistency, this is the definition followed in the present document.

The mechanisms and limitations of best practice research (i.e. of the various methods and approaches in use to identify best practices) have been examined rather extensively in the public policy and management literature[12]. Yet, despite existing methodological shortcomings, the identification and sharing of best practices present important added value from a practical and policy-oriented point of view. Crucially, best practice research enables organisations to learn from others in the same domain and re-use their experiences. Even the investigation of a simple exemplar case may be useful to practitioners if it allows them to get ideas and to solve similar problems they face[13]. In sum, best practice research is a way to generate useful knowledge and to promote the accumulation of experience in a given field.

A **guideline**, on the other hand, is any document that aims to streamline particular processes according to a set routine. By definition, following a guideline is never mandatory (protocol would be a better term for a mandatory procedure). Guidelines may be issued and used by any organisation (govern-

[9] Operational and Technical Challenges of ABC systems (August 2013); ABC summary table (quarterly updates).

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

[11] Council of the EU, EU Schengen Catalogue: External borders control, Return and readmission- Recommendations and best practices, Council document No 7864/09, 19 March 2009, p. 6.

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

[13] Ongaro, E., A protocol for the extrapolation of 'Best' Practices: How to draw lessons from one experience to improve public management in another situation, 2009, available at: *http://epsa2009.eu/files/Symposium/An %20approach %20to %20the %20extrapolation %20of %20practices_EOngaro.pdf* last accessed on 2 June 2015.

mental 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 public and private organisations to reflect that knowledge, typically based on experience, which can be shared in order to achieve improved results towards specific objectives. Along the present document, the term Best Practice Guidelines (BPGs) will be used.

1.4. How to read this document

While these ABC Best Practice Operational Guidelines have been conceived as a standalone resource, ideally they should be read in combination with the Frontex '*Best Practice Technical Guidelines for Automated Border Control (ABC) Systems*' (also known as 'BPTGs').

The present document is structured in two main areas, (1) operational considerations for ABC and (2) traveller experience.

The operational area proposes best practice guidelines and recommendations on:

- operational and functional requirements of an ABC system,
- implementation of an ABC system including the decision-making process, procurement, and cost benefit analysis,
- the deployment of an ABC system with particular emphasis on different topologies and integration in the host environment,
- personnel management, i.e. the roles and tasks of border guards,
- how to handle the most common exceptions.

The traveller experience area proposes best practice guidelines and recommendations on:

- how to create awareness among travellers about an ABC system and educate them on its proper use,
- how to run a high-quality and user-friendly service, and help achieve a satisfactory travel experience.

The document includes a glossary clarifying the terminology used and a list of acronyms. In addition, it is complemented with a series of annexes listing additional reference material and providing an overview of the ABC systems which, at the time of writing, are operational or planned in the MSs.

2. General overview of ABC systems

2.1. Concept

ABC is defined as an automated system which authenticates the electronic machine readable travel document or token, establishes that the passenger is the rightful holder of the document or token, queries border control records, then determines eligibility of border crossing according to the pre-defined rules. Currently, the ABC systems based on the use of an electronic travel document which have been deployed in the MSs rely on facial recognition as the basis for biometric verification, with the exception of France and Hungary, which rely on fingerprints as a primary biometric modality, as well as Spain, Estonia and Bulgaria, which have introduced the fingerprints alongside facial recognition.

The automated border check process starts with e-Passport scanning. The traveller inserts the biographical data page of the passport into the passport reader. The reader checks optical security features, extracts the characters in the Machine Readable Zone (MRZ) and communicates with the chip in the e-Passport to verify the authenticity of the document. A live captured facial image of the traveller is then compared with the one stored on the chip. In some implementations fingerprints are used as the additional biometric identifier[14]. This process is fundamentally the same as in the manual border control booth. Human oversight is provided by a border guard in a monitoring and control station, who supervises the whole process. In addition to the document authentication and identity verification processes, this may include other checks (such as database queries) to verify the eligibility for border crossing. If the process is successful the e-Gate allows the traveller to cross the border. If the process fails, the traveller is referred to manual control.

The use of e-MRTDs (in most cases e-Passports) as the storage medium for travellers' personal data means that no additional biometric registration of travellers is necessary. As such, ABC systems are dependent on the quality and accuracy of data stored in the travel document.

2.2. Main functions and features

In short, an ABC system performs the following tasks (the same ones as in the manual border control) with a high degree of automation:

- Check that the traveller trying to cross the border is carrying a genuine and valid travel document. This is more formally referred to as the 'Document authentication process'.
- Verify biometrically that this travel document belongs to the traveller trying to cross the border. This is more formally referred to as the 'identity verification process'[15].

[14] For additional details on the processes of fingerprint capture and verification please refer to the ABC BPTG.

[15] For further details on the Identity Verification Process, please refer to the ABC BPTGs.

- Check that the traveller is eligible for the system and entitled/authorised to cross the border.
- Allow/deny passage according to a predefined logic, sometimes requiring the intervention of the border guard operating the system.
- Guarantee the security in the overall process, meaning that only a 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). This is typically achieved by the usage of single or double automatic barriers (e-Gates) and tailgating detection/prevention mechanisms.

For the purpose of this document, these are the basic functions that any ABC system must perform. Other complementary or more advanced functions are also possible (e.g. automated profiling, registration of Entry/Exit), but are out of the scope of this document. However, in view of the Smart Borders proposal, processing of third country nationals (TCNs) may be facilitated with the use of ABC systems, thus additional features may be integrated into the ABC[16].

In general, an ABC system involves the use of:

- physical barriers (single-door or double-door e-Gates),
- full-page e-Passport readers: optical recognition of the biographic data page, the MRZ and a radio frequency (RF) reader for communication with the chip,
- monitor displaying instructions,
- biometric capture device,
- system management hardware and software.

The systems may benefit from including uniqueness and liveness detection, i.e. technologies which ensure that only one person enters the e-Gate at a time and that the biometric feature is captured from a 'live' person.

2.3. Advantages of automation

The primary objective of ABC systems MUST be to reconcile traveller facilitation and security. In other words, traveller facilitation is the main objective to maximise, and security a boundary condition that has to be met.

The principal audience of ABC systems are EU, EEA and Swiss citizens (EU/EEA/CH) who according to the Schengen Borders Code are subject to a 'minimum check'[17], with the exception of certain MSs who launched RTPs and/or have the ABC system open for certain TCNs. Accordingly, the 'thorough check' carried out on TCNs may set more requirements on the ABC systems as regards the process (e.g. stamping and visa checking), but the primary objective remains the same.

Cost-effectiveness is also an important dimension to be observed. Properly set ABC systems allow for an increased rate of traveller checks in a given time at first-line control without necessarily having to increase the number of border guards. Moreover, it can be expected that costs will go down when ABC lines become more widespread, while well-trained and motivated operators can further contribute to the effectiveness of the systems.

For every task in the border check process that is modified by the introduction of the

[16] For detailed information on the processing of TCNs with the use of ABC systems please refer to Guidelines for 'Automated Border Control Processing of third country nationals', Frontex, 2015.

[17] 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).

ABC system, it is important to carry out a risk assessment in order to understand how the automation has impacted on existing risks or created new ones, and thus react accordingly.

ABC systems can be equally effective at air, land and sea BCPs. However, their use at land and sea BCPs has to be further explored because of the limited practice among MSs.

3. Operational considerations for automated border control

3.1. Overview of the Border Checks Process

The Schengen Borders Code, the EU Visa Code[18] and national legislation set the framework for the various measures which are implemented at the BCPs of the Schengen Area. The detailed operational model followed at each BCP is carefully designed according to the specific situational requirements, the border check code of practice, the cooperation schemes in place with neighbouring countries and risk analysis, among other factors. Thus, differences are often found from one implementation to another.

The notion of 'border check' means the checks carried out at BCPs, to ensure that a person, including their means of transport and the objects in their possession, may be authorised to enter the territory of the MSs or authorised to leave it. In ABC some tasks are automated and others are carried out by travellers as self-service. As a general principle, there should be no difference in the outcome (i.e. acceptance/rejection) if border checks are automated or carried out in the 'traditional' way. However, it is important to note that automating border check procedures when it is technically feasible with equal levels of accuracy and security allows better use of personnel, e.g. by allocating more resources to check those categories of travellers whose checks cannot be automated. On the other hand, the border check process can be split into several sub-processes or tasks. Each sub-process is an individual part of the overall process.

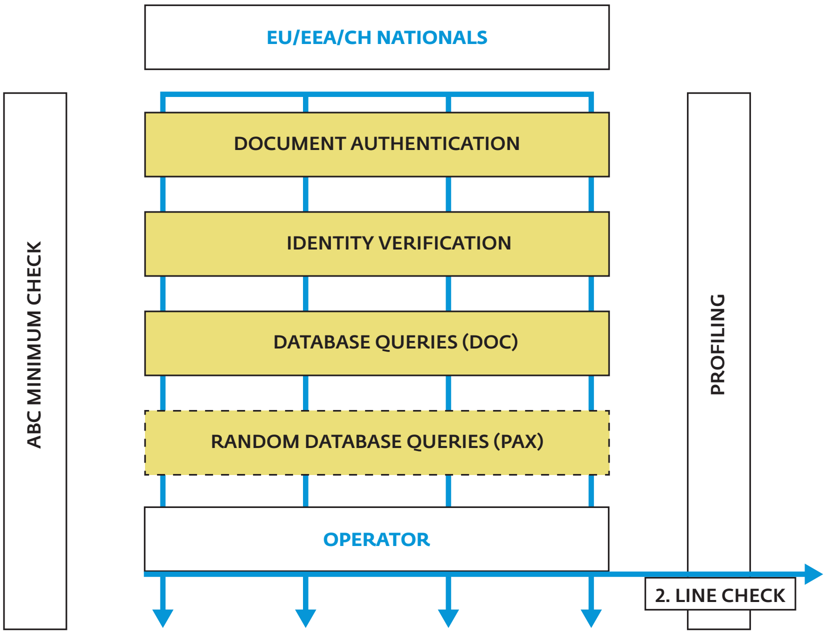
3.2. General process flow

The following flow diagram illustrates a tentative border checks process for EU/EEA/CH nationals. This is presented here for illustration purposes only, in an attempt to provide the right context for the requirements and guidelines hereby proposed. It should not be considered as an explicitly recommended practice since the specific needs of each border crossing point may require a different approach. Moreover, border checks flow for TCNs is different as it includes some additional steps[19].

[18] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code).

[19] Specific aspects of border checks on third country nationals with the use of ABC systems are addressed in the Guidelines for 'Automated Border Control (ABC) Processing of Third Country Nationals (TCNs)', Frontex, 2015.

Figure 1: **Border checks process flow**



The yellow colour indicates the tasks within the process that can be automated by means of an ABC system, hence these will be the focus of subsequent discussion.

3.3. Operational requirements

The following general operational requirements MUST be observed by any ABC system in order to achieve basic operational harmonisation across EU implementations:

1. 'Cold lines' (i.e. stand-alone unsupervised e-Gates) MUST NOT occur. There SHALL always be an operator present who monitors the functioning of the e-Gates[20]. The operator MUST be trained to use the system and also be capable of reacting to malfunctions and to non-cooperative behaviour on the part of the traveller.
2. The operations of an ABC system MUST comply with EU legislation (i.e. Schengen Borders Code) and be compatible with the Practical Handbook for Border Guards (Schengen Handbook) where applicable (e.g. systematic database queries shall not be done on persons enjoying the Community right of free movement except on their travel documents)[21].
3. Before e-Gates can be operational there MUST be an officer ready to operate them. An ABC system MUST be easy to use by travellers, requiring as little guidance as possible. There SHOULD be adequate instructions for the use of the e-Gates.

[20] The Schengen Borders Code (Article 7) explicitly assigns responsibility for conducting checks at the external borders to border guards. Thus, monitoring by an official constitutes a precondition to fulfil legal requirements.

[21] European Commission, 'Recommendation establishing a common 'Practical Handbook for Border Guards (Schengen Handbook)' to be used by Member States' competent authorities when carrying out the border control of persons, C(2011) 3918 final, 20.6.2011.

If ABC systems are complicated or unintuitive to use, travellers will be likely to seek manual lines instead of automated ones.

4. Tailgating MUST NOT be possible. Regardless of whether lines have a man-trap configuration or not, there SHOULD be an automated detection of tailgating to alert the operator.
5. The physical disposition of the area where the ABC system has been set up MUST prevent trespassing. There will be situations when some e-Gates are out of service or the passenger flow does not demand the whole line of e-Gates to be opened. Therefore, a flexible configuration is recommended to ensure a smooth operation of the e-Gate line. The system MUST alert the operator to pay attention when a minor is using an e-Gate. The Schengen Borders Code commands that particular attention SHALL be paid to minors crossing an external border, whether travelling accompanied or unaccompanied[22].
6. Some MSs do not allow minors (i.e. persons under 18) to use e-Gates, but some MSs have no legal basis to refuse them access to automated lines. If minors are allowed to use the ABC system, the border guard operating the gates SHALL carry out a further investigation in order to detect any inconsistencies or contradictions in the information where there are serious grounds for suspecting that they may have been unlawfully removed from the custody of the person(s) legally exercising parental care over them.
7. A risk assessment MUST be undertaken to look at any vulnerabilities in and threats to the system integrity and apply appropriate mitigations.
8. If a traveller is unable, for any reason, to use the ABC, and is redirected to a manual border control booth, due attention MUST be paid to ensure that the ensuing procedures are in full compliance with fundamental rights.

Additionally to the above requirements, the following guidelines SHOULD be considered:

1. The overall traveller throughput of a bank of e-Gates monitored by one officer SHOULD be comparable to or higher than that of a manual booth.
2. As technical failures or breakdowns may happen, contingency plans and procedures SHOULD be in place to inform the travellers, airlines/carriers and all relevant authorities working at the BCP on these measures.

3.4. Functional requirements

This section outlines the process of how travellers are verified by the ABC system. It is not intended to go into specific technical details as these will be dependent on the pre-existing IT infrastructure and are covered, to a much greater extent, in the BPTGs. It is thus included here for context and reference purposes.

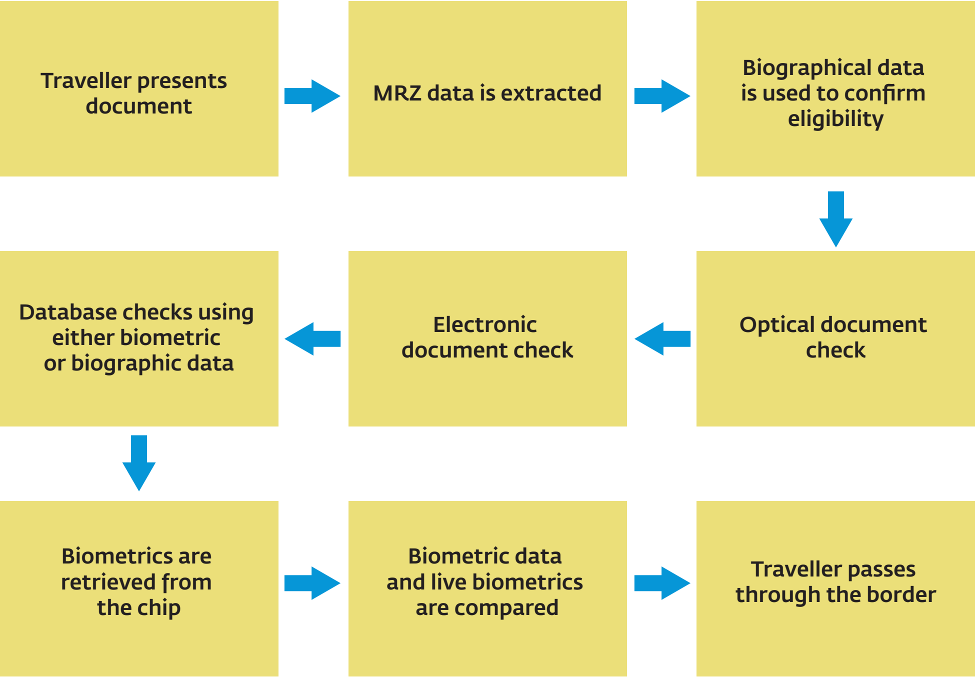
The diagram in Figure 2 sets out the typical process for the verification of travellers using an ABC system. The general principle is that, if travellers fail any of the checks, then either they will be rejected by the system and will see an officer in the traditional manual process, or the failure will be dealt with by the operator and/or the assisting personnel. While in general it is RECOMMENDED that a process similar to the one outlined here is adopted, there are a number of its aspects which are essential. These are indicated in the sections below.

3.4.1. Checking the document authenticity/validity

As noted above, the ABC systems discussed in this document are based on the use of ICAO-compliant e-MRTDs. The process of verifying that the document is authentic and

[22] Schengen Borders Code, Annex VII, paragraph 6.

Figure 2: **ABC process**


Traveller presents document
MRZ data is extracted
Biographical data is used to confirm eligibility
Optical document check
Electronic document check
Database checks using either biometric or biographic data
Biometrics are retrieved from the chip
Biometric data and live biometrics are compared
Traveller passes through the border

valid for use begins with the reading of the MRZ. Once the MRZ has been read, the eligibility of the traveller is determined. Next the system can proceed with the subsequent stages of document authentication. If the MRZ cannot be read successfully the traveller will be rejected and will need to be processed manually by a border guard.

ABC systems MUST carry out multiple checks to confirm that the document is valid and genuine[23], including:

- a verification of the optical security features of the document,
- a verification that the chip in the document belongs to the physical document,
- a verification of the electronic security features of the chip contained in the document.

The optical document check provides some valuable assurance that the document is a genuine one, but it SHOULD NOT be treated as the sole method of verifying the document. The primary check that MUST be carried out is the electronic document check. This will confirm that the chip is genuine and has not been altered, which in turn gives certainty that the biometric data contained on the chip is authentic.

The databases which support the verification of optical and electronic security features need to be updated on a regular basis or otherwise significant numbers of travellers will be rejected as new documents and chips are released. The procedures for conducting such updates are outside the scope of the ABC system but it is essential that a reliable system is in place.

[23] For requirements on the Document Authentication Process, please refer to the BPTG.

3.4.2. Identity verification

3.4.2.1. Biographical data

Since the alphanumerical data extracted from the MRZ is needed to perform the basic access control (BAC) function in order to access the chip in the e-Passport, it is RECOMMENDED that the same data is used in other parts of the process, such as eligibility checks, including database queries, if applicable. It is RECOMMENDED to compare the data in the MRZ with the data in VIZ.

3.4.2.2. Biometric data

The ABC system MUST retrieve the biometric data from the chip in order to compare it with the biometrics captured live from the traveller. If the two sets of biometrics match, the traveller will be able to proceed. The same principles apply regardless of the biometrics concerned.

3.4.2.3. Consultation of databases/ watch lists

The biographical data may be checked against available databases[24]. If there is a potential match then the traveller SHOULD be directed to an officer. The exact process will depend upon the procedures in place within each border management authority.

3.4.2.4. Recording of entry/exit data

Depending upon the implementation, the system MAY allow for the recording of a traveller's Entry/Exit data. For such implementations particular attention should be given to the existing legal framework[25].

3.5. Implementation of ABC system

3.5.1. Decision-making process

It is RECOMMENDED to have a phased approach regarding the decision-making process for the implementation of an ABC system. This is particularly important for MSs which are new to ABC because, although systems are beginning to become standardised and it might seem that they can be bought 'off the shelf', in practice each MS has unique requirements for the operation of their border control and so any system will need to be designed to meet specific demands at the local level. A number of MSs have followed this model and it has helped to avoid costly mistakes later on.

While the process may vary from one MS to another, the following key phases are examined below:

1. ABC Business Case.
2. Cost Benefit Analysis.
3. Risk Assessment and Procurement.
4. Testing Research and Validation, including a Vulnerability Study.
5. Running a Pilot.

By following this process the authorities should be in a good position to take a dependable decision on the ABC implementation.

[24] Additionally, a check against a biometric watch list may be performed offline.

[25] Some MSs, but not all, already record entry and exit data at their external borders. In addition, the EC has announced plans to launch a EU-wide Entry/Exit System as part of the Smart Borders Package (see COM(2011) 680 final).

3.5.1.1. ABC business case

Innovative projects are often dependent on subsidies granted by governmental institutions or provisioned funds by highly involved stakeholders. Before a budget can be committed to the ABC project, however, it is RECOMMENDED to develop a robust business case and to perform a sound cost benefits analysis (CBA).

This section is not intended to go into detail on how a business case for ABC should be constructed, as this will be a matter for individual MSs. Yet it is important to emphasise that the development of a business case SHOULD be the starting point for any ABC deployment. It is critical to identify what the problem is to be addressed by the roll-out of an ABC system. For example, is an ABC system being introduced to clear queues, or increase security? Is it to replace certain functions of the border guard officers or to lower the costs of operations? Is it to provide a visible piece of technology for the travelling public? A clear focus on business outcomes will increase the chances that the system will work effectively and address the key concerns of the border management authority.

ABC deployments have the potential to be politically driven, and if this is the case then one will need to be realistic about what the system can achieve. Political drivers can have a dramatic impact on any business case and this could result in a system deployed without clear requirements at locations where there is no strong benefit. Thus developing a successful business case can provide a clear line of argument in order to convince decision-makers and select among available offers from the market.

Once the business case for the system is clearly defined, it is possible to begin defining how and where the system should be deployed (see section 3.6 for details on deployment).

3.5.1.2. Cost benefit analysis

This is the most critical part of the business planning process. Defining a clear method for calculating the financial benefits of the system is essential as the business case will rely heavily on whether the ABC system delivers efficiencies over the existing manual process. With this in mind it is RECOMMENDED that a detailed analysis is carried out of the cost of operating the manual control as this will provide a good platform for comparison with the ABC system.

The CBA is intended to support the decision-making process, by providing an insight into the differential cost and benefits that come from the deployment and operation of the ABC system against the baseline scenario, i.e. manual checks. A properly conceived and executed CBA facilitates the decision-making process around key questions, like:

- Does it pay off to invest in the project?
- What are the costs and benefits for each stakeholder?
- What are the possible outcomes and their likelihood?
- What uncertainties and risks are really relevant in this project?
- Should we run a pilot first? How much should we spend on it?
- What is the optimal design and dimensioning?
- Should we buy, rent or pay per use?
- What if...?

The first principle of good cost benefit analysis is that it should be honest (e.g. it should not underestimate costs or outweigh benefits, or be specifically tailored to support an already made decision). The second principle is to follow a proven methodology that provides a structured, understandable, efficient, repeatable and low-risk approach.

To foster harmonisation, Frontex has developed a complete framework comprising the tools and data for the modelling, simulation and cost benefit analysis of ABC systems, and may be contacted before embarking in the CBA of an ABC system.

The CBA process SHOULD be structured in four stages:

1. defining the requirements and goals that the CBA will pursue,
2. developing the models that reproduce the system and environment,
3. gathering the data,
4. carrying out a meaningful analysis towards the decisions under study.

The CBA process is one of dialogue that involves at the very least decision-makers, ABC technical and operational experts, and a facilitator who can steer the process and translate the discussion and group knowledge into analytical/modelling/data components. The CBA team MUST include all these stakeholders. Failing to do so will not only ensure that relevant information and perspective are lost, but also that the results will lack the buy-in from the parties being left out.

The requirements and goals for the CBA SHOULD be relevant for the decisions under study. Too often the requirements and goals are unnecessarily detailed, complicating the next stages, making traceability of results difficult and increasing the risk of incurring mistakes.

The models SHALL be no more complicated or detailed than strictly needed for the purposes of the requirements and goals defined in the previous stage. Expert validation is RECOMMENDED, particularly if the analyst is not familiar with modelling and simulation techniques.

It is also RECOMMENDED that the modelling of the ABC system is flexible enough to target the largest possible traveller cohort. By being able to accommodate ID cards holders, partnership arrangements with other countries, minors, visa holders, residents and multiple biometrics the system will be able to respond to changes in business (and potentially legal) requirements and provide greater value for money over the long term. As noted above, flexibility should be embedded into the system so that it is able to accommodate changes.

Using good data is extremely important. Field data SHALL be used whenever possible. In the absence of field data, tentative data from other installations MAY be used. When neither one nor the other is available, or deemed to be not applicable, standard industry benchmarking figures MAY be used. Figures obtained through industry or product catalogues SHOULD be treated with caution.

The analysis stage SHOULD take into consideration the reliability of data and assumptions made. It is RECOMMENDED that a sensitivity analysis is made (using tornado charts) and relevant 'what if' scenarios are analysed. The result of the analysis might uncover aspects that were left out in the definition of the problem, factors that need remodelling or data whose uncertainty needs to be narrowed down. In these cases, the process SHOULD be iterated taking into account the new requirements, knowledge and considerations.

Headline cost of the system has a big impact on the eventual benefits, so a system which has been designed to deliver an agreed outcome will allow cost reduction and innovation. It is therefore RECOMMENDED that the cost/benefit model makes some assumptions on the expected cost, but that the requirements are not so tightly defined so as to result in an increase in cost or that opportunities to reduce cost are missed. A good example of this is the debate over mantrap vs single physical barrier design, where the same outcome was achieved by introducing a range of sensors, reducing space and cost.

3.5.1.3. Risk assessment

It is RECOMMENDED that detailed work on assessing the risks associated with ABC is carried out as part of the planning process. As the technology is relatively new to the majority of border management personnel it is important to capture the attitude to risk and also be open about the potential areas of uncertainty.

It is RECOMMENDED to launch a process of change management in order to support the border management authority personnel in learning to work with the system[26].

Border management authorities have to calibrate technical and operational requirements for the ABC system, e.g. concerning the percentage of biometric match, thresholds and secure data traffic (see the ABC BPTGs for additional details). As regards software risk in terms of malicious software and back-doors, a timely review of the source code with the supplier in RECOMMENDED.

3.5.1.4. Procurement

Determining the manner of acquiring the product

It is RECOMMENDED to set requirements in order to create or reshape a product or components which can be acquired from the market. This can be accomplished by doing research on what the market has to offer, implementing pilots and determining how components need to be adjusted to specific demands. Moreover, one of the challenges in acquiring a product is to come up with a set of requirements that can fulfil the acceptance criteria as defined by the primary user.

In tendering a product there are different choices to be made when it comes to acceptance criteria and to the decision-making process. Governments could tender the product as a whole and make the supplier responsible for an optimised decision-making process on the basis of government demands, or instead could tender the product as a whole and make the supplier responsible for an optimised technical process interacting with self-made decision-making intelligence. One reason for opting for the creation of government decision-making intelligence is that this would allow full control over the actual business rules without having to consult the supplier to make functional changes.

It is RECOMMENDED to decide well in advance on the procurement model which will be used in acquiring the product. This SHOULD be done in accordance with national and EU procurement policy[27], and it may be

[26] The introduction of new technology may create uncertainty and lead to feelings of insecurity among the border guard officers. In this context, the expression 'change management' refers to the strategies adopted by the border management authority to deal with such uncertainty in a constructive way and 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 the ABC system. For example, in relation to the installation of the Dutch system, the Netherlands embarked on a pro-active change management process which focused on fostering open communication through look and feel sessions and encouraged operational feedback by border guard officers.

[27] See in particular Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts (OJ L 134, 30.4.2004, pp. 114–240).

determined on the basis of contracts which already are in place.

Tendering hardware and/or software

A product involving hardware and/or software can be tendered through two different approaches. Governments may choose to acquire the hardware itself and be responsible for creating and servicing the software which steers the decision-making process. However, it should be noted that creating one's own software may be challenging. Another option is to acquire both hardware and software and make the supplier responsible for setting the requirements wanted. In any case it should be ensured that interfaces between the components of the system are stable and tested, and that a responsible entity is designed.

When it comes to deciding on the tendering process, there may be a closed tender with a pre-selection stage in order to determine which companies are qualified, on the basis of experience and reliability, to provide a complete offer and receive classified information.

A tender based on a sound list of requirements should provide governments with a qualitative product. Besides the qualitative aspect, getting a cost-beneficial product should obviously be a major goal of tendering.

Elaborating the Terms of Reference

In setting requirements it is advisable to generate internal studies to define functional and technical demands based on security processes and traveller flows in the designated area. Doing research in a real life environment can also supply valuable information as to the criteria which the product should meet. Support regarding the creation of a tender document for the definition and tendering phases could be provided by external and/or internal experts.

In order to warrant the acquisition of a product which fulfils key requirements, it is RECOMMENDED to formulate knock-out criteria regarding technical and functional requirements with which the supplier has to comply. Any non-compliance should imply exclusion from the tendering process.

It is RECOMMENDED to ask competitors to provide information on performed field tests (if available) regarding experiences with the implementation of the e-Gates or similar systems.

In the end all offers need to be ranked on the basis of the tender criteria according to the offered prices, with a lower limit in place to avoid 'dumping' practices. These may happen if offers are ranked only by the lowest price, which means that in the ranking criteria price has more value than qualitative criteria. Thus, it is RECOMMENDED to set up a pricing model which duly includes the quality standards that have to be delivered. For example, a 100 per cent total score could equal 40 per cent price and 60 per cent quality requirements as defined by knock-outs and options.

The tender documentation shall fulfil legal requirements and the tendering process be clearly defined, both in order to ensure transparency and to minimise any chances of lawsuits. The time it takes to tender can vary depending on which body is tendering and on how the process is being managed[28]. The overall time for having a complete tender, including the time devoted to the creation of requirements and to the actual tendering until the signing of the contract, can be more than one year.

The duration of the contract is dependent on the type of product/service which has been

[28] Public, private or public-private partnership.

tendered. Different possibilities exist regarding what to tender: (1) to tender the product so that it will be the property of the tendering body, (2) to tender the product as a service. The latter means that the tendering body will not add property to its inventories but will engage into a service management contract with the supplier based on a Service Level Agreement.

The service management model offers flexibility to generate various service management levels for ABC systems. In certain areas there might be a need for enhanced service management or better performance depending on flow pressure or on the wear off time. Moreover, with this model it is possible to introduce changes to the ABC system without having to purchase all new components when there are innovations in the market or when multimodal techniques are to be installed. Additionally, in this regard, issues such as obsolescence and parts replacement should be taken into consideration. It is RECOMMENDED that these issues are regulated in advance in the contract. Currently in some MSs it is a practice to include in the contract, for example, stipulations regarding development of new algorithms or performing software updates.

Evaluating proposals

Before implementing the ABC system, validation procedures SHOULD be developed and executed by the primary user of the systems, both from the functional/operational and technical sides. All installations need to be subjected to these tests as part of the acceptance process.

Formulating and managing Service Level Agreements (SLAs)

There are different approaches to the formulation of SLAs:

- SLAs which concern services of the supplier should be formulated as part of the tender documentation.
- SLAs concerning helpdesk services, incident management and energy support should be managed in a governance framework. When such a framework is already in place, an SLA may be incorporated into it.
- SLAs can also be managed as part of the activities of a Support Unit within a government department (ITIL, Service Operation). In this case, a flexible communication framework should be put in place to make sure that this Support Unit can operate effectively, especially when more than one government body is involved in the provision of technical and/or functional support.

Operational, tactical and strategic levels should be clearly defined and responsibilities should be allocated to the different bodies and suppliers taking part in the SLA framework. When systems are operational and SLAs need to be managed it is RECOMMENDED that SLA criteria are agreed upon in a formal manner and are measured and controlled according to the responsibilities formulated in the framework. Failure to address this issue would entail the risk of disputes at later stages.

3.5.1.5. Testing research and validation

Before running a pilot, it is RECOMMENDED that the authorities carry out a market consultation and related research in order to have a clear overview of the present and future possibilities available in the market.

After a market consultation has been performed, a request should be addressed to different suppliers for the purpose of testing their systems. Testing is important because, when tendering a product in the future, governments should be quite certain that the requirements set will result in acquiring flexible and easily adjustable systems.

Once a clear view of the market possibilities has been developed, the authorities should consider having a pre-pilot-testing research or benchmarking phase with different systems and designs. A testing-research phase may assess the dimensions outlined in Table 1 below.

It is RECOMMENDED that the authorities make a final report on the performance of each of the systems tested. By comparing the results outlined in such reports, it should be possible to choose the system(s) which will be implemented as a pilot. The most important of all the aspects considered should be the system's overall stability, security and service management.

3.5.1.6. Running a pilot

It is RECOMMENDED that any large-scale installation be preceded by a pilot phase to identify key issues and implement improvements. A pilot phase allows the MS to evaluate the design and performance and fine-tune it before committing to a large-scale deployment, while ensuring that the tender requirements are met. Implementing a pilot is crucial to ascertain how stability, service management, interfaces and security processes are performing. Furthermore, environmental aspects, mainly lighting and the IT infrastructure, can impact on the performance of the system and thus need to be observed and tested.

A pilot would also allow validation of the new border process. In order to work with ABC systems and use them as a proper tool in servicing travellers border guards have to familiarise themselves with the system functionalities and such functionalities have to be tested in the operational environment.

Table 1: **Testing-research phase dimensions**

	Dimension	Focus
1	Installation	Physical characteristics of the product, eg. Does the product consist of a single-door e-Gate or of a double-door e-Gate; of one or more fixed cameras or a moving one?
2	Design and operational ability	System design, materials and usability from the perspective of the traveller and of the border guard.
3	Usage of sub-products	Components being used in the ABC system: the document reader, the biometric capture unit, the biometric verification unit, etc.
4	Compatibility	Various possibilities regarding interfaces and architecture.
5	Speed	Speed of the system as a whole and if possible of the different sub-processes.
6	Accuracy	Biometric performance.
7	Stability	Overall stability of the system and its different components, and service management performed.
8	User acceptance	Experiences with the product from different perspectives, including from the perspective of the border guard, high-level immigration officers, the traveller and the port operator.
9	Security	Security aspects of software and hardware as well as their flexibility and the possibilities for adjustment. The security aspect should also take into consideration the securing of the data processed by the system as well as system itself. Vulnerability assessment should be performed.
10	Service management	Requirements for technical, configuration, security and incident management. The service management dimension should also encompass the helpdesk and problem management levels as well as the procedures to escalate issues when they cannot be solved at a certain level.

The white-hat vulnerability and penetration testing[29] is RECOMMENDED during the pilot and it should also be repeated on a regular basis in post implementation. White-hat testing must be carried out by an independent third party with access and expertise to carry out the tests properly. It should include both systems and physical security tests.

The systems installed in the pilot phase will have a certain design and Man Machine Interface (MMI). This MMI is as key for travellers as it is for border guards in creating a smooth process. Testing the MMI is critical and will help in sharpening the requirements, as border guard officers and travellers will be able to provide feedback and describe their experiences in interacting with the system.

Acceptance of the system by border guards is crucial for its successful operation. Explaining the technical aspects and processes of ABC system will increase confidence, which can be instrumental in change management strategies with a view to strengthening the process and the speed of innovation.

3.5.1.7. Taking a decision

By following the various steps of the phased approach described above, the border management authority and the cooperating third parties, if applicable according to the financial arrangements specific to a certain implementation (see Section 3.5.3. on cooperation with third parties), should be in a position to take a well-informed decision on the implementation of an ABC system which is tailored to their requirements.

3.5.2. Equivalence of performance

ABC systems have allowed border management authorities to analyse processes and decision-making in greater detail. Experience has shown that the principles of biometric comparison are not well understood, and for this reason it is RECOMMENDED that senior managers within the border management authority are educated on the principles of ABC functioning and on key concepts such as False Accept Rate (FAR) and False Reject Rate (FRR), as this will increase their understanding of the limitations of the system and increase their confidence.

Implementations of the ABC systems have highlighted the need to understand the facial verification performance of officers, which is unknown, and this prevents a fuller comparison of how ABC systems perform in relation to the traditional manual alternative. An academic study assessing the performance of ABC systems in the operational environment would contribute to filling this gap in our collective knowledge. It is also RECOMMENDED that MSs carry out biometric performance tests of the implemented biometric systems[30].

3.5.3. Cooperation with third parties

There are two main groups who need to be effectively engaged besides the border management authority: the port operator and the relevant carriers, on the one hand, and the supplier of the ABC technology, on the other. If successful engagement with these two groups is achieved then the border management authority will be more likely to see high levels of take-up by the travelling public.

[29] White-hat testing (or white-hat hacking) is penetration testing performed by a computer security specialist aimed at ensuring the security of information systems. It is performed as 'breaking into'/attacking the system or network.

[30] In this respect one may refer to the BSI TR-03121-3.1 Technical Guideline Biometrics for Public Sector Applications. Part 3: Application Profiles and Function Modules, Volume 1: Verification Scenarios for e-Passport and Identity Card, Version 3.0.1.

3.5.3.1. Working with the port operators, carriers and other agencies

The border management authority MUST have strong levels of support from the port operator to achieve success. The e-Gates SHOULD be situated in a prominent location (see section 3.6.4 on integration in the host environment), and have good signage and way-finding information. In most cases this will demand some physical restructuring of the port environment, and this cannot be achieved without the support of the port operator.

Additionally the port operator is the primary point of contact with the carriers serving the port, so they have a major role to play in making travellers aware of the ABC system prior to their arrival. Finally the port operator is also in a position to make a tangible contribution to the ABC system, either in the form of financial support or a partnership agreement, or by providing customer service personnel to assist travellers on how to use the system[31].

3.5.3.2. Working with suppliers: Service Level Agreement

The supplier has the most important role to play in ensuring that the system is trouble free, as they are responsible for guaranteeing that it operates as intended and is kept in service. The SLA (see section 3.5.1.4. on procurement) with the supplier MUST be clearly defined, and cover any sub-contractors. In particular it is RECOMMENDED that:

- response times, fix times and penalties are explicitly defined, and a workable service management framework is established to enable faults to be reported quickly and accurately;
- personnel operating the service desk are educated on ABC to increase their understanding of the system;
- officers are trained to troubleshoot problems on site to keep e-Gates operational;
- the supplier is transparent about the level of engineering coverage – this is particularly important if there are multiple sites;
- there is a defined schedule of maintenance to reduce the number of failures;
- reliability is ‘designed in’ by ensuring the system is as modular as possible, with the fewest number of moving parts;
- there are regular stakeholder/supplier forums;
- there is a defined change control mechanism.

3.6. Deployment of ABC system

3.6.1. Topologies of ABC system

In general there are three topologies of ABC systems in use. The WG has agreed on the following terms to describe each configuration:

- **One-step** process which combines the verification of the traveller and their 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. Please refer to the Figure 3.
- **Integrated two-step** process, which is a variation on the one-step design described above. The difference between the two topologies is that in an ABC system designed as an integrated two-step process the traveller will initiate the verification of the document and the traveller’s eligibility to use the system at the first stage, and then if successful move to a second stage where a biometric comparison and other applicable checks are carried out.

[31] Within the context of this BPG, ‘customer service personnel’ refers to staff of the port operator who are tasked with providing guidance, advice and assistance to travellers in using the ABC system. Some MSs use the term ‘hosts’ to refer to this personnel.

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

Alternatively, a segregated two-step process may be implemented/configured in a way allowing for its reconfiguration into a one-step process topology with virtual mantrap (depending on the circumstances) with the use of the same devices and software, i.e. reconfiguration from a segregated two-step process to a one-step process and back.

Figure 3: **One-step process with mantrap**

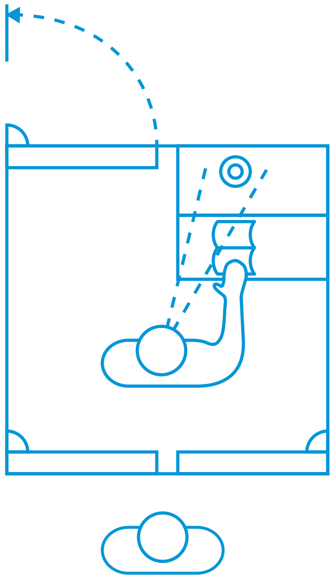


Figure 4. **Integrated two-step process with mantrap**

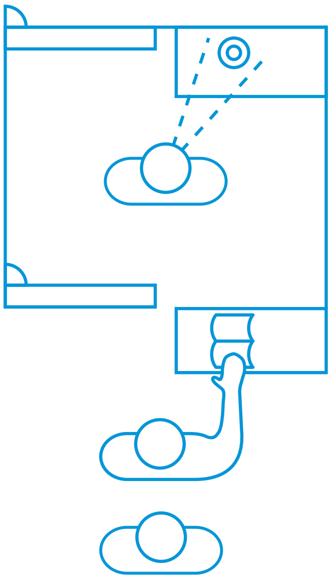


Figure 5: **Segregated two-step process – Step 1: Biometric Verification and Document Authentication**

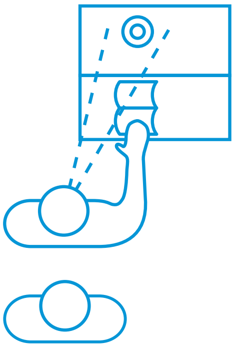
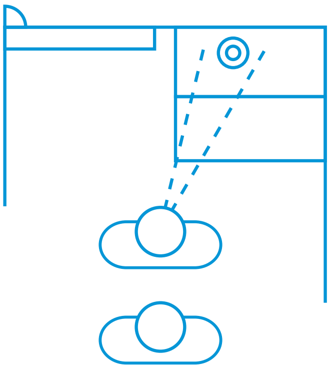


Figure 6: **Segregated two-step process – Step 2: Biometric Token at the e-Gate**



3.6.2. Physical infrastructure: arrangement of the e-Gates and the monitoring and control station

Queuing lines for the e-Gates SHOULD be located next or close to the queuing lines for manual checks. Very often it is difficult for inexperienced travellers to orient themselves towards the correct queuing lines, be they manual or ABC. If the wrong line is chosen by accident it SHOULD NOT be too complicated to reach the intended line. Some synergy on operations can also be achieved when manual and automated lines (EU/EEA/CH) are situated next to each other. In particular, this eases the pulling of travellers from the manual queue to the ABC system by customer service personnel (see 4.2.3. on 'managing traveller flow').

The monitoring and control station may be built in a way so as to allow manual first line checks. A possible approach is to build the monitoring and control station like a control booth for two manual lines. One post is for the operator and the other for their assisting personnel (see section 3.7.1. on the roles and tasks of personnel). If an incident occurs that requires further inspection or an interview, the system will prevent the traveller from proceeding and indicate what to do next. The monitoring and control station may have the same equipment as manual lines and MAY also be used as two manual lines in the case of an ABC system being out of service (e.g. due to system crash, repair or maintenance). Additionally, an open e-Gate (functioning as a queuing funnel) with a supervisory booth could serve as a manual checking point.

3.6.3. Environmental factors

This section sets out the factors which should be considered when deciding on the physical location of the ABC system.

In the early stages of the implementation there will probably be constraints (for example in relation to existing infrastructure, cabling, hardware design and lighting) affecting where the system can be installed, as the ABC will have to be accommodated within the existing border control arrangement.

Yet it should be noted that the location of the system will play a large role in determining how many travellers use it, how successful it is and what level of performance can be achieved.

3.6.3.1. Location requirements

The location of the ABC system should be accessible to everybody but will be partly dictated by the size of the hall and the prevailing traveller flow. It is RECOMMENDED that the system is placed:

- **In front of the existing manual control.** Placing the system behind the manual control has a detrimental effect on traveller usage. MSs have observed that in those installations where, due to space constraints, the e-Gates were placed behind the manual control stations, the system was left unused and this resulted in poor customer satisfaction and wasted resources.
- **In a highly visible and prominent location.** It is essential that the system is visible to travellers as soon as they enter the hall. If travellers enter from a variety of locations then the system should be sited to favour the prevailing traveller flow. In some MSs ABC systems were placed at the far end of the hall, and whilst this was better than situating them behind the manual control lines, it impacted on usage as travellers tended to turn to the manual lines closer to the entrance.
- **Alongside the manual lines (EU/EEA/CH).** This will allow the travellers who are queuing for the manual lines to observe the users of the e-Gates, which will pro-

mote further usage of the system and allow self-education to take place.

Consideration should also be given to the location of the monitoring and control stations. A number of options are available, such as behind the system, alongside it, or in an elevated position overlooking it.

It is RECOMMENDED to place the monitoring and control stations behind the ABC system in order to enable their use as first line control booths if the ABC system is out of service (see section 3.6.2. on physical infrastructure). That way the traveller will still go straight ahead and will not need to be redirected. On the other hand, the chosen location of the monitoring and control station may be dictated by the space available in the hall.

Whatever location is chosen some account should be taken of the potential need to relocate the stations in the future. A flexible configuration is RECOMMENDED so that this can be accomplished at a minimum cost.

3.6.3.2. Environmental lighting conditions

It is RECOMMENDED that environmental factors such as strong electric lighting, variable daylight or illuminated advertising boards are also taken into account when positioning the ABC system. This is particularly relevant for systems based on facial recognition where variable lighting due to daylight can trigger performance issues with travellers being 'silhouetted' by strong background light, which may result in high numbers of rejections. This challenge was experienced by some MSs.

3.6.4. Integration in the host environment

It is RECOMMENDED that the system is integrated into the hall to contribute to the smooth flow of travellers through the border control. Ideally such integration should take place in such a way so as to allow for the expansion of the system if traveller usage increases. This will facilitate the gradual move of travellers from the manual process towards the automated lines.

3.6.5. Flexibility to accommodate changes

3.6.5.1. Optimal dimensioning of the system

The number of e-Gates available for travellers will vary with the flow rate to be processed and the service quality delivered. For any given amount of traveller flow[32], more e-Gates will reduce queuing time but at the same time will use more resources (financial, material and human) and will complicate the monitoring, support and risk profiling tasks. There is an inherent trade-off between service excellence and cost-effectiveness that needs to be carefully balanced.

One way to determine the right dimensioning of the number of e-Gates is by means of operational research. A queuing analysis, either analytical or by simulation, will reveal the relationship between the three variables: 1) flow rate, 2) service quality and 3) lifecycle cost, and will allow for the identification of bottlenecks, resource consuming elements and optimal trade-offs.

A possible way to carry out such analysis is as follows:

- The flow of travellers is examined.

[32] Please note that the traveller flow varies during the day, during the week and per season; queuing varies on the ratio of eligible and non-eligible passengers as well as willingness to use the system and if one family member cannot use the system (like minors) the whole family might choose to be non-eligible. The above aspects should be taken into consideration when a business case for an ABC system is developed.

- A service quality Figure of Merit (FoM) is defined (e.g. queuing time).
- A desired value is chosen for this figure of merit (e.g. less than 5 minutes for 95 % of travellers)[33].
- The traveller flow is stochastically characterised (e.g. arrival rate as a log-normal distribution).
- An operational model is developed observing different arrangements and number of e-Gates.
- A lifecycle cost model is developed for the different arrangements and number of e-Gates.
- A FoM and lifecycle cost are calculated for all possible combinations of arrangements and number of e-Gates (e.g. using discrete event simulation and Monte Carlo simulation[34]). Combinations failing to meet the security threshold or other equivalent criteria are automatically discarded at this point (i.e. only points in the Pareto frontier are considered).
- Dominant configurations providing the best FoM for any given lifecycle cost are drawn in a curve FoM vs Lifecycle Cost. This is the cost-effectiveness Pareto efficiency frontier of the system.
- A point in the curve, and thus a specific arrangement and number of e-Gates, is chosen on the basis of available budget and comparison with manual checks.

The method described above can also be used with minor modifications to forecast the tipping point when an already operational implementation might need to be upgraded, and even to simulate the effect on service quality of possible modifications.

It should be noted that in some cases the experience has shown that the assumptions on the usage of e-Gates will be changed when e-Gates are put into operation. Therefore, it is necessary to review those assumptions in the context of the identified discrepancies affecting the CBA. The following assumptions of usage may deviate from expectations: the number of actual e-Gate users, the false rejection due to inappropriate FRR threshold settings and the percentage of irregular cases that warranted further manual inspection.

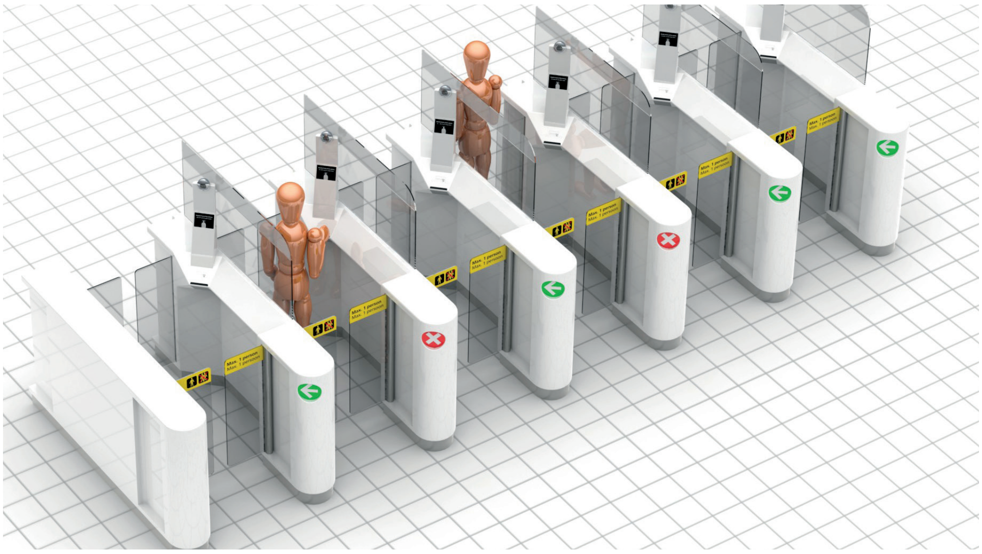
In addition, the planned deployment should take into account the anticipated use of the ABC system in the future. For example it is estimated that by 2016 all EU/EEA/CH passports will contain chips[35], and so at that point it could be reasonably expected that all passport holders will be aware of the ABC system, with the vast majority being capable of using it. With this in mind the system SHOULD be designed in a modular fashion which will allow it to be expanded, and located in a way so that such expansion can be achieved with a minimum of disruption and cost. A carefully designed system, which maximises the throughput capacity and minimises the processing time, will be able to support increased traveller volumes. The figure below illustrates a modular system.

[33] See the IATA 'Airport Development Reference Manual'.

[34] Monte Carlo simulation is a computerised mathematical technique that allows an accounting for risk in quantitative analysis and decision-making. Monte Carlo simulation performs risk analysis by building models of possible results by substituting a range of values – a probability distribution – for any factor that has inherent uncertainty. It then calculates results over and over, each time using a different set of random values from the probability functions. Monte Carlo simulation produces distributions of possible outcome values.

[35] Under Regulation (EC) No 2252/2004 of 13 December 2004, MSs were required to begin issuing e-Passports by August 2006. Assuming a maximum period of validity of passports of 10 years, the rollout of e-Passports could then be completed by 2016 at the latest (see COM(2008) 69 final, 13.2.2008.

Figure 8: **Modular ABC system**



3.6.5.2. Flexibility of configuration

The degree of flexibility is dependent on the configuration chosen for the ABC system. A description of the possible topologies is presented in section 3.6.1.

3.6.5.3. Physical relocation

As the lifetime of the system can span over five years it can be reasonably expected that the e-Gates will need to be relocated at some point during that time. A MS found that within 18 months the e-Gates at one of their sites needed to be moved in order to allow the arrivals area to be refurbished at considerable expense in both time and money. It is RECOMMENDED that the system is designed in such a way so as to allow it to be relocated at minimal expense and effort.

Full mobility MAY NOT necessarily be needed – one of the MSs has experimented with a mobile design but ultimately decided that they did not need this full functionality. Mobility can be achieved by designing a system that will connect wirelessly (note: wireless connection is not allowed in some MSs due to IT security requirements) and securely to the IT infrastructure and one that can be deployed without extensive drilling or other building work. However, it should be noted that rules and regulations may require an electrical appliance to be firmly fixed in order to comply with the applicable safety requirements in place.

3.6.5.4. Reliability

This can be covered to some degree by the service levels that are in place with the supplier (detailed in section 3.5.5.2.), but it is RECOMMENDED that systems have reliability 'designed in', with a minimum of moving parts and integration of established and trusted components to reduce the number of failures. It is also RECOMMENDED to establish maintenance schedules to ensure reliability.

Some MSs have experienced some reliability issues early in their installation lifecycles, whereas others have had few issues reported.

However, the experience has shown that a dust-free environment for the e-Gate equipment is very important, as the dust may affect the document readers and other parts of the system. Practice has shown that to ensure a dust-free and easy-cleaning environment it is recommended to place ABC systems on marble/stone/tiled floors which are better to prevent the build-up of dust and fibres as opposed to, for example, carpets.

Additionally, having easily replaceable components is RECOMMENDED in case of failure (e.g. passport readers which can be removed and replaced without affecting the entire system).

3.6.5.5. Fall-back solution

A fall-back solution MUST be in place in case the system fails. This is particularly relevant in the early stages of an installation, or if the design is untested. As the technology matures it is expected that the need for a full fall-back solution will diminish, as suppliers will learn which factors contribute to good reliability.

Yet it is anticipated that this trend will ultimately reverse if automation becomes the primary method of checking travellers at the border control, because the traditional fall-back response of deploying border guard officers instead will no longer be feasible as officers or manual control booths may not be available in sufficient numbers. In any event, the border management authority needs to develop a reliable fall-back solution to guarantee that border checks continue to be conducted smoothly regardless of the system.

3.6.5.6. Business Continuity

It is RECOMMENDED that all MSs who install and operate an ABC system have a business continuity plan in place in case of a major incident which affects the system's operational use. The plan will reflect the dependency MSs have on the system and the effect this will have on overall passenger processes.

The primary contingency solution if the ABC system fails is to send passengers to the manual control desks. In future, as MSs become more dependent on ABC systems there may not be enough manual desks or staff to process passengers within set service standards. If this is the case then other contingency plans will need to be found. This can range from the re-deployment of staff from elsewhere to improving the resilience of the system so that there are back-up servers and connectivity which can be utilised in the event of a major failure (this will necessitate the need for well-defined disaster recovery plans for the ABC system and increased costs for additional IT capability).

3.7. Personnel management and ABC systems

3.7.1. Roles and tasks of personnel

There are two main roles in the operation of an ABC system: the one of operator and that of assisting personnel. Other roles are also possible, although these two are the ones common to every ABC system in place at the time of writing.

3.7.1.1. Operator

The operator is responsible for the remote monitoring and control of the ABC system. The most important task of an operator is to bring the necessary human factor into the automated tasks. With unattended standalone lines it is impossible to reach an acceptable level of facilitation and border security.

An operator:

- monitors the user interface of the application;
- reacts upon any notification given by the application;

- manages exceptions and makes decisions about them;
- communicates with the assisting personnel for the handling of exceptions at the e-Gates;
- monitors and profiles travellers queuing in the ABC line and using the e-Gates to look for suspicious behaviour in travellers. Note however that this is also among the responsibilities of assisting personnel (see below);
- communicates with second-line checks whenever their service is needed.

Operators do their job through the user interface of the control application located at the monitoring and control station. This SHOULD be positioned so as to allow the operator to monitor travellers at the ABC lines (e.g. in an elevated position or equipped with CCTV). When monitoring queuing travellers, the operator SHOULD evaluate the traveller flow in order to detect suspicious behaviour and to identify travellers who should be more closely checked. The evaluation or assessment method is typically based on a traveller's actions and body language, i.e. non-verbal communication. The process to follow depends on the local implementation and integration of the ABC system with the border control procedures.

An operator MUST NOT[36] leave his post when the e-Gates are active[37]. If human intervention is required at the e-Gates, the operator should first alert the assisting personnel to handle it (e.g. to assist a traveller in a mantrap).

In normal circumstances when the traveller flow is continuous without pauses, the maximum surveillance time for an operator SHOULD be no longer than 30 minutes. The operator and the assisting personnel MAY change their tasks at intervals of 20-30 minutes. If there are natural pauses in the traveller flow (e.g. because of flight schedules) or if the frequency of the traveller flow is moderate an operator MAY work for periods longer than 30 minutes.

The operator and the assisting personnel MUST be linked with a communication system if they work separated from each other.

3.7.1.2. Assisting personnel

The assisting personnel are the border guard(s), whose tasks are to handle the exceptions that take place at the e-Gates, redirect travellers as needed and assist travellers on specific situations. Assisting personnel work in close cooperation with an operator.

Assisting personnel may have the following tasks:

- handles exceptions and assists the operator;
- carries out short interviews in order to find out if it is necessary to redirect a traveller to a second line check;
- makes traveller assessments and informs the operator. For instance, they profile travellers queuing in the ABC line and using the e-Gates, and look for suspicious behaviour among travellers;
- escorts travellers to second line checks when needed;
- conducts manual checks at the first line of border control if the ABC system fails;
- informs and provides on-the-spot support to travellers (e.g. families, minors);
- assists persons with disabilities.

Every operator MUST have assisting personnel available.

[36] However, in exceptional circumstances, in particular in case of emergency (e.g. if someone needs immediate assistance) the officer could leave the post.

[37] Human supervision constitutes a prerequisite to fulfil legal requirements under the Schengen Borders Code (see section 3.3. on operational requirements).

The location of the assisting personnel highly conditions the time they will spend in each of the above tasks. Placing the assisting personnel behind the e-Gates will make them focus mainly on handling exceptions and assisting the operator, whereas being located in front of the e-Gates will make them spend more time in assisting travellers and profiling.

3.7.1.3. Number of e-Gates supervised by an operator

During field tests it was observed that a single border guard can typically supervise from three to 10 e-Gates. Those tests were carried out on inbound flow (travellers entering the territory of the MS operating the ABC system).

There are limitations as to how many e-Gates an operator can supervise in practice. Those limitations are due to the limited ability of human beings to concentrate on several things at the same time. It is therefore important to assess how much attention the operator needs to devote to stay focused. The number of e-Gates that one operator can monitor is inversely proportional to the level of attention (and therefore energy) required for maintaining a good and thorough situational awareness.

There are some known aspects that condition the maximum number of e-Gates that can be reliably controlled by an operator. These are among others:

- the quality of face recognition, and automatic liveness detection as well as the amount of human intervention required;
- the frequency of the traveller flow and how busy the system is;
- whether the e–Gates are located at entry or exit checks;
- the profile of the traveller flow at the BCP, what is the ratio of own nationals and other EU citizens, and how often operators have to react and channel travellers to manual first-line or second-line checks;
- the design of the user interface at the operation desk and how much information the operator has to process and the amount of human intervention required;
- the reliability of the system;
- the proficiency and training of border guard officers.

The above-mentioned factors MUST be considered and analysed when deciding the number of e-Gates to be simultaneously supervised by an operator. With time, when the system has proved to be reliable and the operators have familiarised themselves with it, this number may be adjusted.

Experience has shown that one operator should not monitor more than seven e-Gates on arrivals or more than ten on departures. The table below summarises the ratio of operator to e-Gates in a number of MSs with operational ABC systems. The average number of e-Gates per operator currently sits at five, so it could be argued that this has been established as being the most effective level at present. One MS has introduced a flexible approach whereby the operator manages fewer e-Gates at peak hours, but more at periods of low traffic. This allows the system to stay open and available without committing extensive numbers of operators.

The key factor in increasing the e-Gate to officer ratio is the amount of data sent or displayed to the operator. If this can be reduced and/or simplified by automating more steps of the process, only displaying the most important information, or by reducing some of the functionalities, then the officer may be able to be responsible for more e-Gates. This may be achieved by accessing less important data through pop-ups or other means when it needs to be viewed. It is important to understand that the information necessary for Border Control responsibilities should not be removed, rather the data displayed should be simplified.

Table 2: **Number of e-Gates per operator in selected MSs**

Country	e-Gates per operator
Finland	5–10
France	3
Germany	4–6
Netherlands	3
Portugal	7
Spain	6
UK	5

The operator's interface SHOULD be designed in such a way that it can be easily split into two or more monitoring and control stations in order to quickly accommodate new operators into the task.

3.7.2. Training of personnel

Training is an essential component of the successful implementation of an ABC system, and it is RECOMMENDED that a detailed analysis of training needs is carried out before the system goes live. It is recommended to develop common EU training for different levels of expertise so as to cater and ensure common training standards and knowledge in this area.

Areas that SHOULD be considered are as follows:

Change management and internal marketing

Because of the likely impact that the introduction of an ABC system will have on operational staff, managers will need to be adept at managing change and direct the integration of the new border control process at their BCP. The staff will also need to be properly informed and educated on the system and its purpose, since a positive approach from all involved plays an important role in the success of the implementation. Pro-active change management to engage staff and manage their concerns has proven successful in reducing resistance to the introduction of the ABC implementation.

Operational training for the officers

The skills and personal aptitudes of officers vary a great deal and it is possible that some will not be immediately comfortable with the introduction of the new technology. Initial and follow-up training will be required so that officers can operate the system successfully and contribute to its enhancements.

Expert user training for a select number of officers

Expert users are those who are able to bridge the operational environment with the technical infrastructure. It is RECOMMENDED that the border management authority educate a sufficient number of expert users to assist in providing additional ad hoc training. These officers can also be used to troubleshoot problems and diagnose faults, acting as a first line of defence against technical issues. MSs' experience indicates that introducing expert users early in the installation has effectively contributed to develop local expertise within the border management authority staff.

3.8. Handling of exceptions

Border guards need detailed instructions on how to proceed when specific exceptional situations occur.

There MUST be a modus operandi handbook (e.g. ABC Handbook for Border Guards) providing detailed instructions on how to proceed with the various unwanted/unexpected situations that may present themselves at ABC e-Gates. Those measures SHALL be decided in advance and SHALL be exercised through practice by operating personnel. Provisions SHALL be made to ensure that all forms of unwanted/unexpected situations can be avoided or effectively neutralised. Chosen measures may vary at different BCPs depending on the infrastructure, the number of e-Gates, the frequency and the profile of the traveller flow.

The following section introduces a compilation of RECOMMENDED measures to deal with a set of commonly encountered situations involving exceptions. Specific instructions MUST be tailored according to the particularities of each implementation.

3.8.1. System malfunctioning

If there is a disruption in the normal operation of the system (e.g. power shutdown, communication outage, component failure, random errors), there are typically two possible ways forward: the first one is to open one or two e-Gates and perform manual checks at the supervision station, which is the default recommended option. If that is not possible, the e-Gates SHALL be closed and checks be carried out at the manual first line.

When establishing contractual agreements with suppliers or when developing the own service system, it is RECOMMENDED to define service quality agreements.

3.8.2. e-Gates out of service

If one or more e-Gates are out of service while the rest operate normally, there MUST be an option to physically close those e-Gates in order to prevent travellers from inadvertently trying to use them.

3.8.3. Tailgating

If two persons try to go through an e-Gate at the same time, they MUST be stopped, the reason for the behaviour clarified and the travellers processed accordingly.

3.8.4. Minors

Manual checks are RECOMMENDED for families with small or several children who are unlikely to be able to use the e-Gates independently or assisted. If minors (under 18 years) are allowed to use e-Gates, there SHOULD be information available on the procedures, e.g. on the minimum height required and on the fact that e-Gates must only be passed by one person at a time under all circumstances.

If a traveller enters an e-Gate with a child in his arms, they MUST be stopped and redirected for manual checks.

3.8.5. Travellers with disabilities

Currently, ABC systems do not provide full access for all travellers with disabilities. This particularly applies to persons with limited mobility, such as wheelchair users, those who are unable to stand unaided, visually impaired or those who cannot provide the required biometric.

It is RECOMMENDED that the design of ABC systems takes into consideration all categories of persons with disabilities as well as the elderly and is adapted to cater for them to the greatest possible extent (keeping in mind the business case for the implementation). Therefore, the ABC systems' ergonomics, dimensions, location and the environmental conditions SHOULD be considered with a special focus on the needs of travellers with disabilities. In particular, the following is RECOMMENDED[38].

[38] The recommendations included in this section are based on the input from the European Disability Forum.

- The location of the ABC system in the terminal is accessible to everybody.
- Adequate signage is used (e.g. floor guidance systems, tactile 'footprints' on the floor, tactile and standardised signage for blind people). The signage is harmonised throughout the EU.
- If possible, the information before entering the e-Gate is available in different formats (e.g. audio information, big print, easy-to-read).
- If the environmental and practical aspects permit (e.g. level of noise), audio instructions during the border check process at the e-Gate are provided.
- Adequate lighting and size of visual feedback are ensured, allowing travellers with visual impediments to use the e-Gates independently.
- Wider gates allowing for the use by travellers on self-propelled wheelchairs are accessible. (Such gates have already been installed in the UK, while Germany is currently running a pilot at the Hamburg airport[39]).
- The passport and fingerprint scanner/camera are installed at a height which is easy to reach for everyone, including persons of small stature and wheelchair users.
- It is ensured that the e-Gate doors do not close on travellers, especially if they move slowly or if they have difficulties with orientation due to a disability or old age.
- An intercom is available in order to alert assistance, especially if the area is very crowded and it is difficult to communicate.
- All groups of staff are provided with adequate training as regards the needs of persons with disabilities, how they can be assisted efficiently and discretely.
- Close cooperation among the disability movement, the suppliers and the authorities responsible for ABC system implementation is in place with regard to all phases of the implementation process as well as elaboration of any guidelines in this respect.
- Accessibility requirements are detailed in the tendering procedure which is in line with EU public procurement legislation.

It should also be noted that in EU MSs as a general rule travellers with disabilities are provided with special services and have priority to go through the manual border control.

3.8.6. Trespassing

The infrastructure at ABC lines and the surrounding site SHALL be such so as to prevent trespassing. If trespassing happens despite the measures in place, there MUST be a practised modus operandi to quickly react and catch the trespasser. Methods may vary at different BCPs from patrols to remotely controlled doors.

3.8.7. Ineligible travellers

The design of the e-Gate process MUST ensure that those travellers who are not allowed to use the e-Gate based on their nationality, the document issuance country and age are rejected by the ABC system and redirected to the appropriate manual control lanes[40]. Moreover, the eligible travellers who cannot use the e-Gate because of physical constraints should be provided with adequate information and assistance.

[39] However, the usage thus far has been low.

[40] As part of the Smart Borders package, the EC is planning to present a legislative initiative to establish an RTP which would allow certain groups of frequent travellers (e.g. business travellers, family members) from third countries to enter the EU, subject to appropriate pre-screening, using simplified border checks at automated gates. It is foreseen that this could speed up border crossings for 4 to 5 million travellers per year (see COM(2011) 680 final).

3.8.8. e-Passport is wrongly placed into the reader

When a traveller places the e-Passport onto the reader in the wrong way, information SHOULD be provided about the correct way to handle this transaction. Information can be provided through a system screen (see section 4.2.1. on instructions at the e-Gate), a voice command from the operator or through hand-to-hand guidance by the assisting personnel or by other customer service staff.

3.8.9. Non-cooperative behaviour at the e-Gate

Non-cooperative behaviour at the e-Gate may occur when, for example, a traveller moves too much during the face recognition stage, looks in the wrong direction or stands in the wrong place. In such situations, advice SHALL be given to the traveller on how to proceed. If this has no effect, the person SHALL be directed to manual first line checks.

3.8.10. Anomalies in chips

Some e-Passports may be rejected by e-Gates. This will happen for instance when these are not fully ICAO 9303-compliant genuine travel documents, containing so-called 'defects'. This is the case when the public key is missing, the certificates have expired or there are some other technical issues[41].

If a chip is broken or cannot be read for some other reason, a traveller SHOULD be redirected to a second line for more thorough checks on the travel document. Anomalies SHOULD be considered as a red flag indicating a possible risk situation[42].

3.8.11. Database hit

If a database hit occurs and requires intervention, the traveller SHALL be redirected to the second line check.

3.8.12. Failed biometric verification

In the case of a failed biometric verification the operator – depending on the outcome of biometric verification – should decide how to proceed (some systems allow the Border Guard monitoring the gates to accept a passenger who has failed facial recognition and allow them to proceed). The traveller MAY be redirected for manual identity verification and to a second-line check as necessary.

3.8.13. Wrong or no security features on the biographical data page

The biographical data page SHALL be checked with visual light, UV light and IR light. The system MUST be configured to check for and detect irregularities in the security features. If a security feature is missing or some other hints suggest that the document may be false or forged, a traveller SHALL be redirected to a second line check.

[41] For further information, please refer to Frontex, 'Discussion paper on Public Key Infrastructure (PKI) and operational challenges of certificate exchange/management at the borders', 14.6.2012.

[42] See Frontex, 'Operational and Technical security of Electronic Passports', July 2011, section 2.5.4 on security issues. However, please note that according to Article 4 of 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, as amended by Regulation (EC) No 444/2009 of 28 May 2009, 'the failure of the matching in itself shall not affect the validity of the passport or travel document for the purpose of the crossing of external borders'.

3.9. Quality assurance and statistics

Part of the planning process concerning the set-up of an ABC system consists of defining what information needs to be retrieved from the system itself. Such information may comprise the operational data needed in the form of statistics as required by the border management authority or by other stakeholders, and the technical data required for quality assurance. These data will also contribute to the continuing process of enhancing the business case discussed earlier and the cost-efficiency of the system.

The requirements for information retrieval must be defined together with other operational requirements as they have an impact on the technical implementation of the system. The specifications should define the categories of data to be saved and the basic data processing rules, i.e. where the data is saved, for what purposes, who has access to it, the retention time and what information is to be logged on the usage of the system. This information should be included in the technical documentation of the ABC system provided by the contractor after – or as part of – the tendering procedure, and it may be used later to fulfil the legal requirements applicable in relation to the provision of information on the processing of personal data.

For statistical purposes, it is RECOMMENDED to use a minimum amount of anonymised data, such as nationality of the traveller, for each transaction. Storage of personal data identifying the traveller, including the passport number, SHOULD be avoided without proper justification.

Quality assurance is a process by which 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 the border management authority.

Quality assurance is important when assessing the performance of a given ABC system, as it helps identify potential problems in its operation and also feeds back to development of exception-handling procedures. For the purposes of quality assurance and performance measurement, a variety of data may be needed, for instance the temporary storage of the facial images captured live during the verification process.

The storage and usage of this kind of personal data should be very limited, and sufficient safeguards MUST be in place to protect the data. Other data can be collected to obtain key performance indicators, enabling the supplier and the border management authority to carry out comparative analysis.

The present BPGs focus on the minimum recommended anonymous operational data to be collected for quality assurance and for the extraction of business statistics in ABC systems. ABC systems are subject to the same privacy and data protection requirements and legislation as applicable to any other system entailing the processing of personal data.

For more details on the quality assurance, refer to the BPTGs, section 6.

4. Traveller experience

The main goal of an ABC system should be the facilitation of cross-border traffic. The design of the system and the provision of education and information to travellers are essential to ensure that they have a positive experience when using it.

ABC systems, as they currently stand, provide a similar service to travellers, although there are a number of differences between implementations not only in appearance, but also in functionality and usage. This lack of universality makes the task of harmonising the expectations and usability a difficult one. The novelty of such systems (while obviously decreasing with time) is another major challenge. Many eligible travellers will be unfamiliar with the relevant concepts and steps of the process, particularly since implementations tend to differ. In order to provide a successful traveller experience, attention must be devoted in particular to:

- creating awareness and educating travellers before their arrival to the e-Gate, and
- ensuring that the ABC system provides a user-friendly service.

The following sections offer a number of recommendations, drawing on operational experience and surveys conducted by some MSs to achieve the objectives outlined above. However, other approaches may be found to accomplish similar results.

4.1. Awareness and education before the e-Gate

Delivering information before the traveller arrives to the e-Gate is challenging.

- Since it is given in advance, only a limited amount of information will be retained. Travellers may not remember detailed usage instructions for a long time.
- Such information does not have the visual support of the real system or of other users using the system; hence interpretation may vary significantly from one individual to another.

It is RECOMMENDED that any information given in advance be oriented towards creating awareness of the system and developing willingness to use it. The earlier this information is given, the simpler it has to be in order to be effectively retained.

4.1.1. Key messages to be transmitted

Making the traveller aware that an ABC system is available and can be used for their own benefit is critical to getting more travellers to leave the queue for the conventional manual control. Information provided in advance SHOULD convey the message that it is better to use ABC than to opt for manual border checks. Only if a considerable number of travellers use the system will the investment be justified.

The process of providing education before the e-Gate can be usefully divided into the following categories:

- understanding the BENEFITS that the system brings to users,
- communicating that the system is EASY to use,
- communicating that it is POSSIBLE to use the e-Gate at the BCP,
- explaining who is ELIGIBLE to use the e-Gate,
- describing HOW to use the e-Gate.

The latter category overlaps considerably with the aim of providing information on usage at the e-Gate, but can also differ, being aimed at different aspects of the process such as instructing travellers about what signage to look for in order to find the e-Gate, the queuing process and the preparations required to use the system (e.g. have the e-Passport ready).

4.1.2. Delivery methods

The following methods have been used at the different ABC implementations to deliver these messages to the travellers:

- signs ('airport' format)/logos,
- videos,
- human assistance (either ahead of the e-Gates or at the e-Gate),
- leaflets,
- posters/banners,
- literature (a page in in-flight magazines),
- audio announcements,
- online information.

The locations in which this is done include:

- on aircraft,
- in waiting/transit areas (this could include lounges, walkways and baggage handling areas),
- on port's website.

No formal assessment has been carried out yet on the effectiveness of the different methods used. Moreover, there is currently no uniform signage at ABC systems in operation in the EU, which will be detrimental to the public understanding of such systems.

It is RECOMMENDED that:

- a study be conducted to establish the most effective ABC awareness-raising methods,
- the target audience be carefully analysed, and the best methods be chosen according to the specifics of this audience. It is also important to remark that the composition of this audience will vary in time and thus the methods of choice will also have to be modified accordingly[43].

Other public information methods exist which have not yet been tried by some or all MSs, and are worth considering. Examples include:

- an EU-wide awareness-raising campaign. This will become more cost-effective when ABC systems are extended to land BCPs, where opportunity for pre-border education is limited or non-existent,
- videos on aircraft (and other vehicles),
- 'live' demonstrations by staff in appropriate areas,
- literature provided at issuance of e-Passports.

4.1.3. Need for standard signs, instructions and logos

Signs and any other form of graphical display are very important. They are often the first contact that the traveller has with the system, and to a large extent may condition their willingness to use it.

MSs currently using or piloting ABC systems have tried several different types of signage but none has proven to be clearly more effective than the rest, probably because the concepts e-Passport and ABC are not widely known even among frequent travellers. One of the key challenges lies in developing a set of signs and standard terminology that can be understood by the majority of the travellers[44]. These have to be intuitive for travellers to assimilate them, uniform across MSs and easily deployable.

[43] Currently, these issues are being examined with the framework of FastPass – an EU FP-7 project.

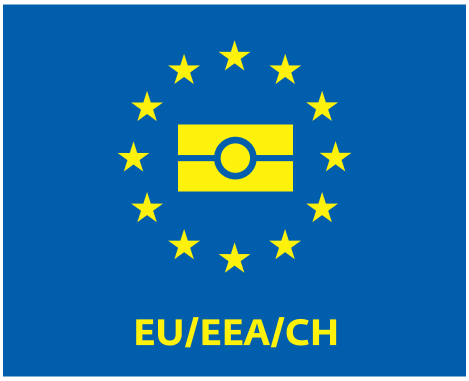
[44] At the time of writing, the UK implemented the 'FaceSymbol' Project, which aims at establishing a standard set of symbols for use by passengers on ABC systems based on facial recognition at UK ports of entry.

In order to facilitate and harmonise the travellers' experience, common signage and instructions are instrumental. While the Schengen Borders Code and the Practical Handbook for Border Guards spell out the common signage to be used for manual checks at the EU external borders (for example to segregate lines for EU/EEA/CH citizens from those for TCN), no similar provisions currently exist for ABC.

In the absence of a common name for referring to the ABC system, the following name is RECOMMENDED in order to denote the existence of automated border control lines: **Self-Service Passport Control**. The name of choice MAY be used in conjunction with a short brand 'catchy' name for the service (e.g. EasyPASS in Germany).

In the absence of a common and unique logo depicting the system, the following logo is RECOMMENDED in order to denote the existence of ABC[45]:

Figure 9: **Recommended ABC logo**



4.2. Running a traveller-friendly service at the e-Gate

Service excellence involves encouraging travellers to use the system, helping them understand that they are eligible, and facilitating a successful transaction. This section outlines a number of recommendations based on operational experience on how to make an ABC service as user friendly as possible.

These are broken down into six areas:
1. instructions to travellers on the usage of the system,
2. effectiveness of the information delivery methods,
3. managing the traveller flow,
4. learning by observation,
5. travellers' interaction with the e-Gates,
6. support to help travellers use the service.

4.2.1. Instructions at the e-Gate

Travellers' cooperation at the e-Gate is essential in order to ensure good performance of the system, a positive experience for all the users, and continuous and accrued use of the e-Gates in time. Clear instructions are thus paramount, and human behavioural factors should be taken into consideration when designing the control process and assessing the overall performance of the system. One MAY consider providing audio instructions at the e-Gate, as long as the environmental factors (e.g. level of noise) permit and the solution will not cause confusion for the average traveller.

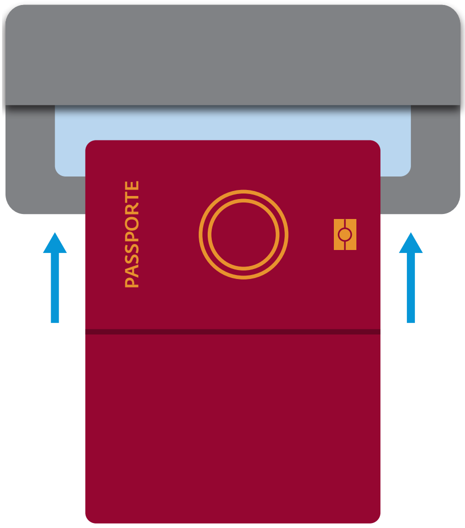
Instructions SHOULD be carefully crafted according to the specifics of each implementation.

It has been consistently observed that the most challenging part of the process relates to the correct placing of the e-Passport by the traveller. The way this step shall be handled is easily misunderstood, and if the document is incorrectly placed then this would

[45] Note however that the only official signs indicating lanes at border crossing points are those regulated in the Schengen Borders Code, Annex III.

almost inevitably result in a failed transaction. Thus, this practical aspect MUST be prioritised when designing instructions at the e-Gate. Clear instructions with an animated display on the screen have proven helpful (see Figure 10 for an illustration).

Figure 10: **Graphic instruction – how to place the e-Passport**



Another recurrent issue is that, during the face capture process, the traveller sometimes does not know when to stop looking at the camera. Thus, some feedback MUST be provided. Visual feedback is preferred to audible feedback as sounds from adjacent e-Gates may create confusion and increase the exception rate (please refer to section 4.2.6. for further information).

'Footprints' on the floor indicating where the traveller should stand in front of the camera may help the traveller to position themselves in the appropriate location for face capture. They may however be counterproductive, as some users concentrate on the footprints and look down instead of looking straight into the camera.

Regarding fingerprints, it has been observed that travellers sometimes have difficulties in placing the finger(s) in the way which is required for capturing images of the best possible quality. Thus, it is RECOMMENDED to provide visual instructions indicating how the fingers should be positioned, as well as feedback in the event of bad-quality capture. When instructions are provided in an audible form, the tone and volume SHOULD be regulated to avoid confusion with sounds from adjacent kiosks or e-Gates.

4.2.2. Effectiveness of delivery methods

There are a variety of delivery methods that can be used to show travellers how to interact with the e-Gates. These range from signage and informational videos to graphics displayed on the e-Gates themselves.

Signage on how to use the e-Gates must be clear and carefully placed for maximum impact. One solution is to provide a step-by-step series of images within the queuing zone allowing travellers to see the sequence of the e-Gate operation. Any video animations should be at or just above eye level and these should reflect the process in a clear and unambiguous way.

Signs SHOULD rely mainly on graphic images and include as few words as possible. While most ABC owners noted that simple graphics work best, it should be taken into account that some icons mean different things to different cultures. Complex sentences are not easily understood and SHOULD be avoided.

For instructions on how to use the system, still images and animations have proved to work better than video. The reason is that the viewer has more information to process when watching a video, and a 10-second video simply adds an additional 10 seconds to the transaction process, which is ineffective.

It has been concluded that informational videos being shown around the e-Gate area often remain unnoticed and travellers do not seem to fully assimilate them. It is possible that these would become more effective once usage rises to the extent that travellers have to queue to use the e-Gates, as then they will be more likely to observe the informational videos whilst queuing.

Audio announcements in the arrivals hall are also considered no better than average in raising traveller awareness.

Leaflets have been used to raise awareness with some success. The challenge with leaflets lies in identifying the most appropriate area for distribution so that travellers are receptive to reading them.

4.2.3. Managing traveller flow

Traveller flow can greatly benefit if it can be assisted by trained personnel in order to have a smooth, uninterrupted flow avoiding unnecessary delays.

It is RECOMMENDED that officers or customer service personnel provide on-the-spot support for queuing users and help distribute the traffic among the different e-Gates. It has been observed that travellers tend to be more receptive when personnel in this role do not wear uniforms.

Travellers holding travel documents not recognised by the ABC system SHOULD be directed to manual border checks as early as possible. Some sites have clearly segregated areas for queuing for the e-Gates. This has been found to be effective as it enables travellers to see the e-Gates clearly.

Strategies used to encourage travellers to use the e-Gates have included the use of signs distributed along the queuing area, and having customer service personnel actively seeking eligible travellers from the manual border control queue. The queuing area SHOULD be designed according to the specific layout and available space of each implementation to enable travellers to choose the queues. In some implementations queues can cross each other. This allows for better usage of floor space, but during rush situations may lead to conflicts between queuing travellers.

4.2.4. Learning by observation

Queuing contributes to the learning process as non-experienced users can observe how other travellers interact with the system. This is an important aspect that needs to be considered when designing the queuing space at the e-Gates.

Within the first period after the installation, the system MAY be configured for the complete process to be slightly slower than strictly necessary in order to facilitate this 'learning while queuing' process. The effectiveness of this measure will depend on a number of other factors, like visibility, usability and previous understanding of the system.

The size of the screen SHOULD be large enough for the user to interact easily AND for the user queuing behind to observe the whole process.

There is some evidence that non-experienced users tend to use the e-Gates closer to their queuing line, that is, the specific e-Gates upon which the observation process took place, as this reduces the feeling of uncertainty. Experienced users, on the contrary, tend to use the e-Gates at the edges. As experienced users generate fewer exceptions and have a somewhat shorter processing time (e.g. the face capture process is faster if the traveller knows how to look properly into the camera) than inexperienced users, the e-Gates at the edges may exhibit more throughput and fewer exceptions than the ones closer to the queuing lines, despite being exactly the same in terms of hardware, software and configuration.

4.2.5. Traveller interaction with the e-Gates

The screens used to display the graphics vary in size, but generally a larger screen works more effectively, particularly if it is large enough to be observed by the travellers queuing to use the e-Gates. Screens SHOULD be tuned to be readable in all lighting conditions. If this is not the case, their effectiveness will be reduced.

Processes where the traveller simply goes forward rather than having to turn or alter course were considered to be most effective. It is RECOMMENDED that the design allows the traveller to move simply forward in a straight line, rather than having to turn or stop during the transaction process.

A camera mounted straight ahead has been observed to be more effective than one where a traveller has to turn their head 45 degrees or more. Where the e-Gates are offset to allow for this, travellers would benefit from an audio cue prompting them to exit the e-Gate area.

Audio cues, such as soft 'pings' encouraging the travellers to move to the next stage of the process MAY be used. In the absence of other indication, some mechanical noise is RECOMMENDED to allow the traveller to realise that the e-Gate has actually opened. Whenever audio feedback is given, there SHOULD be acoustic isolation between e-Gates to prevent confusion or false feedback.

In one-step designs where all the transactions take place inside the mantrap (i.e. e-Passport reading is not required to enter the mantrap), it is RECOMMENDED to give a 'Have your passport ready' message in order to avoid that travellers look for their documents inside the mantrap. This can cause unwanted timeouts and frustration among travellers.

The design and the size of the e-Gates (width and length) SHOULD be planned with consideration for the usage of trolleys and other luggage (e.g. duty free bags). Trolley bags are not easily catered for, and problems may occur even at the e-Gate with the largest secure zone (measuring 90cm × 200cm). This is because travellers handle their bags in different ways, and trailing bags can easily obstruct the doors closing, which slows down transaction times.

Unicity and tailgating prevention SHOULD be carefully designed. A number of methods exist to ensure that only the cleared traveller actually goes through the e-Gate. However, this is an area where research is ongoing.

4.2.6. Use of text and multiple languages

In general it is RECOMMENDED that the use of text in any instructions to travellers is as far as possible kept to a minimum. This is because travellers find it difficult to process information when presented in this way, particularly if they are unfamiliar with using an automated system.

Some countries outside the EU rely more heavily on the use of text, but this is often the result of the system purpose. For example in the Australian case, the ABC system (SmartGate) also performs a customs function whereby travellers have to complete a number of declarations during the process.

In the UK and NL systems the language of the passport holder can be used after the MRZ is successfully read. Therefore, the messages such as 'Take your passport' once the transaction is complete or 'Please see an officer' if the passenger needs to be referred to manual inspection are displayed in the language of the passport holder (determined from the MRZ). This functionality has received positive feedback from travellers.

It is RECOMMENDED that:

- the use of text is minimised as far as possible, with graphics and short animations being used instead (see section 4.2.2. on the effectiveness of delivery methods)[46];
- where text is used, messages are kept short, to a few simple recognisable words or phrases, e.g. 'stop' or 'thank you';
- if text is used, the language MAY be determined based on the nationality in the MRZ or the language options available MAY be limited to that of the host country and English.

4.2.7. Human support at the e-Gate

All new sites installing ABC systems SHOULD include the use of customer service personnel or in some cases of assisting personnel, depending on the method chosen, to show travellers how to use the e-Gates, as this has proved highly effective in reducing the 'fear factor' for first-time users, and educating travellers more successfully than passive techniques such as signage. After the traveller has used the system once, it is generally not necessary to show its functioning again. This means that over time the need for staff members tasked with showing travellers how to use the e-Gates will be reduced. Such effect is likely to be reinforced by the installation of more ABC systems across Europe as the technology becomes more widespread.

Where human support at the e-Gate is provided, the relevant personnel SHOULD be wearing civilian clothing, as travellers find them less intimidating and more approachable (see section 4.2.3. on managing the traveller flow). Many of the operational sites use customer service personnel provided by the port operator.

In some instances operators have requested the installation of an intercom which would enable them to communicate directly with e-Gate users from the monitoring station. Yet, communications between the traveller at the e-Gate and the officers SHOULD be kept to a minimum in order to automate the process as much as possible and minimise the interactions between the traveller and the border guard, as these may slow down the flow. Intercoms may be installed to interact with the traveller under specific circumstances (e.g. 'the door is open, please proceed'). If used, communications SHOULD be initiated by the officer, not the traveller unless there is an emergency. The preferred language options for verbal communication are the local language(s) and English.

4.3. User-friendly design of the e-Gate

4.3.1. System design

The ABC system SHOULD be designed so that it can be operated effectively by both border guards and travellers. Even if the system has been constructed so that process concerning verification and database checks are clear (see section 3.4. on functional requirements), the ability of travellers to use the system easily and effectively will have a critical impact on its levels of usage and on the volume of rejections yielded.

[46] However, UK experience shows that in two areas a short text message improves the passenger process flow: 1. 'Try Again' when a placement error occurs; and 2. 'Take Passport' at the end of the transaction. Although both messages are currently displayed in English only, they have been found to be very beneficial. In the absence of these messages, passengers often seem not to understand the graphics on their own, which slows down the flow.

4.3.2. Attractiveness and safety

The system SHOULD be designed so that it is attractive to travellers – if it is too austere then travellers may find it intimidating and will be discouraged from approaching it for the first time. Consideration SHOULD thus be given to those factors which make the system more inviting, for example:

- there is some evidence that mantrap e-Gates are less inviting than single e-Gate or kiosk systems;
- smoked or darkened glass has a similar effect and clear glass should be used if possible;
- ideally human support at the e-Gate should be provided by personnel who are not in uniform (see section 4.2.7. on human support at the e-Gate).

Safety is also a necessary consideration and local legislation in this area MUST be observed when designing the system. In particular, trip hazards should be avoided, and any doors should be extensively pressure tested to ensure travellers are not hurt if they are caught in them. Doors should also have a fail-safe system so that uncontrolled closure on travellers is rendered impossible.

4.3.3. Ergonomics

Consideration SHOULD be given to ergonomics as these will impact on usage and transaction times. For example:

- e-Passport readers should be at a height which makes them easy to reach by the majority of travellers (average elbow-height), and placed on the right-hand side of the e-Gate.
- Any system should require the minimum essential number of physical interactions. This will reduce the number of times that a traveller has to pass their luggage from one hand to another. The system should take into account the prevalence of large trolley bags carried by travellers.
- If the system has a self-adjusting camera then its default height setting should be configurable so it can be later set to the average traveller height.
- Using graphics with multiple colours or harsh contrasts should be avoided to enable travellers with visual impairment to use the system easily.
- The range of camera heights (minimum and maximum height) should be as wide as possible to enable more travellers to use the system.
- Enhancements such as blinking lights or soft tones to attract the attention of travellers at critical stages should also be considered.

4.4. Privacy and data protection

This document does not make specific recommendations on how to comply with privacy legislation as such legislation varies widely across MSs. However the development and implementation of any ABC system MUST observe privacy and data protection legal obligations in the host country, as well as under the Council of Europe and EU legal frameworks.

The main EU legal instrument on data protection is Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[47]. In January 2012 the European Commission proposed a data protection reform package consisting of a Data Protection Regulation[48], meant to replace the Data Protection Directive, and a General Data Protec-

[47] OJ L 281, 23.11.1995, p. 31–50.

[48] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25.1.2012.

tion Directive[49], providing for data protection in the areas of police and judicial cooperation in criminal matters. At the time of writing this BPOG, discussions on the proposed Data Protection Regulation were ongoing.

In addition, the right to protection of personal data is encompassed under the rights protected under Article 8 of the European Convention on Human Rights[50], which guarantees the respect for private and family life. This provision is closely mirrored by Article 7 of the EU Charter on Fundamental Rights[51]. The Charter also establishes a right to data protection under its Article 8, specifying that such data must be processed only for specified purposes.

The European Data Protection Supervisor (EDPS) recommends that the key data protection principles of 'Privacy by Design' (i.e. embedding privacy in all elements at the early start of the deployment of a system) and 'Privacy by Default' (i.e. building the activities in the most privacy-friendly way by design) are taken into account when analysing and identifying the requirements for the development of a border management system involving the processing of biometric data[52]. These principles should be applied to the design and implementation of ABC systems, taking due consideration of the fact that, unlike RTPs, ABC solutions based on the use of e-passports do not store travellers' personal data but only anonymous operational data for the purposes of quality control and the extraction of business statistics.

[49] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25.1.2012.

[50] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, available at: http://www.refworld.org/docid/3ae6b3b04.html [accessed 4 March 2015].

[51] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

[52] Opinion of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), 18 July 2013.

Annex 1: References

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

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

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

European Commission. *Communication from the Commission to the European Parliament and the Council: Smart borders – options and the way ahead*, COM(2011) 680 final, 25 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 Commission. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final, 25.1.2012.

European Commission. *Recommendation amending the Recommendation establishing a common 'Practical Handbook for Border Guards (Schengen Handbook)' to be used by Member States' competent authorities when carrying out the border control of persons* (C (2006) 5186 final), 20 June 2011.

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

European Data Protection Supervisor. *Opinion on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)*, 18 July 2013.

European Union Agency for Fundamental Rights. *Annual Activity Report 2012*, June 2013.

European Union Agency for Fundamental Rights. *Annual Activity Report 2013*, June 2014.

European Union. *Charter of Fundamental Rights of the European Union*, OJ C 326/02, 26 October 2012, pp. 395-406.

European Union. *Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts*, OJ L 134, 30 April 2004, pp. 114-240.

European Union. *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 amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC*, OJ L 158, 30 April 2004, pp. 77-123.

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 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code)*, OJ L 243 of 15 September 2009, pp. 1-58

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).

Federal Office for Information Security (BSI). *BSI TR-03121-3.1 Technical Guideline Biometrics for Public Sector Applications. Part 3: Application Profiles and Function Modules, Volume 1: Verification Scenarios for e-Passport and Identity Card, Version 3.0.1.* 2013.

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

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

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

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

Frontex. *Guidelines for Automated Border Control Processing of Third Country Nationals*, June 2015.

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

IATA. *Airport Development Reference Manual (ADRM)*, 9th edition, January 2004.

ICAO. *A Primer on the ICAO PKD 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. *Guidelines for electronic – Machine Readable Travel Documents & Passenger Facilitation*, Version – 1.0, 17.4.2008.

ICAO. *MRTD Glossary* [last accessed on 2 June 2015].

ISO/IEC 2382-37:2012, *Information technology – Vocabulary – Part 37: Harmonized biometric vocabulary [ISO2382-37].*

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

PricewaterhouseCoopers. *Technical Study on Smart Borders; Final Report.* October 2014.

Royal Netherlands Marechaussee. *Change Management & Man Machine Interface*, Presentation in the 5th Workshop on Automated Border Crossing Systems based on Facial Recognition and Electronic passports, London, 31 March 2011.

UK Home Office. *'FaceSymbol' Project – Design, development, testing and ISO adoption*, Contribution to ISO/IEC JTC 1/SC 37 on Biometrics, 11 June 2012.

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

Annex 2: Overview of ABC systems in the EU/Schengen Area

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

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

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

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

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

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

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

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

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

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

FRONTEX

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

Plac Europejski 6
00-844 Warsaw, Poland

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

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

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

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