FRONTEX

Technical Guide for Border Checks on Entry/Exit System (EES) related equipment

EUROPEAN BORDER AND COAST GUARD AGENCY

Legal notice

This technical guide was initiated under Regulation (EU) 2016/1624 of 14 September 2016 on the European Border and Coast Guard, and shall be published and implemented under Regulation 2019/1896 of 13 November 2019 on the European Border and Coast Guard Agency.

Frontex – European Border and Coast Guard Agency
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

Warsaw, May 2021, version 1.0
Research and Innovation Unit
European Border and Coast Guard Agency reference number: 8104/2020

PDF:
TT-03-20-651-EN-N
ISBN 978-92-9471-415-2
doi: 10.2819/814713

FPI: 20.0076

Contents

List of figures

List of tables

All rights reserved

Before citing this document, the following procedure should be observed:

1. Please contact the European Border and Coast Guard Agency Research and Innovation Unit in order to get the latest version of the technical guide and support for using it in your document.

In the introductory part of your document:

2. Include a brief text declaring that the *Technical Guide for Border Checks on Entry/Exit System (EES) related equipment* has been used in the document. Mention explicitly which sections in the document are (totally or partially) based on these.
3. Explain briefly why the *Technical Guide for Border Checks on Entry/Exit System (EES) related equipment* have been used, and in case of total or partial use of particular sections, explicitly state why they are copied in full and what the added value is. Provide some background about how using the *Technical Guide for Border Checks on Entry/Exit System (EES) related equipment* best serves the purpose of the document.
4. Briefly mention that the European Border and Coast Guard Agency's *Technical Guide for Border Checks on Entry/Exit System (EES) related equipment* is the result of a collaborative effort between EU Member States (coordinated by the European Border and Coast Guard Agency).

In the body of the document:

5. In those parts of the document based on the *Technical Guide for Border Checks on Entry/Exit System (EES) related equipment*, make a reference to the European Border and Coast Guard Agency document (see references below).

In the references section:

6. Include a proper reference to the European Border and Coast Guard Agency's *Technical Guide for Border Checks on Entry/Exit System (EES) related equipment* (title, version and issuing date, ISBN reference, plus a link to the European Border and Coast Guard Agency web page hosting the latest version).
7. Include European Border and Coast Guard Agency Research and Innovation Unit contact data at the end of the document.

For the above purposes, please use the information below.

Research and Innovation: Standards and Capacity Development
Capacity Building Division
European Border and Coast Guard Agency
Plac Europejski 6, 00-844 Warsaw, Poland
Tel. +48 22 205 9625
SCD@frontex.europa.eu

About the European Border and Coast Guard Agency

The mission of the European Border and Coast Guard Agency is to support the European Union in the application of measures relating to the management of the external borders by reinforcing, assessing and coordinating the actions of Member States (MS) in the implementation of those measures. As such, the Agency plays a key role in analysing and defining the capability needs in border control and in supporting the MS in development of these capabilities. Furthermore the European Border and Coast Guard Agency also provides qualified expertise to support the EU policy development process in the area of border control.

A core objective of the Research and Innovation unit of the Capacity Building Division (CBD) is to drive the process of harmonisation and standardisation, whereby the European Border and Coast Guard Agency has a mandate to define and support the development of technical and operational standards[1] for border control.[2] The role of the Standards and Capacity Development Sector (SCD) is thus instrumental in steering the development, maintenance and promotion of European best practices, technical guides and standards (both technical and operational), providing technical assistance and developing new capacities in support of MS, Third Countries and EU policies related to border management. It requires cooperation and engagement at the national, European and international levels.

1 Since the European Border and Coast Guard Agency is not a standards certification authority, the standards referred to in this document include non-normative technology standards, best practices and recommended guidelines.

2 Article 10(z) and 64(4)(5) of Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13November 2019 on the European Border and Coast Guard.

Acknowledgements

This document was prepared by the Research and Innovation Unit (RIU) of the European Border and Coast Guard Agency in close cooperation with selected external experts from 10 Member States who were engaged at the time of writing in the implementation of Entry/Exit System at national levels, the EU Agency for the Operational Management of Large-Scale IT Systems (eu-LISA), Joint Research Centre (JRC) and selected internal business units of the Agency.

The European Border and Coast Guard Agency would like to acknowledge the work of the external experts contributing from the Bulgarian Border Police, Czech Foreign Police, Dutch Directorate-General for Migration, French Ministry of the Interior, German Federal Police and German Federal Office for Information Security, Italian Polizia di Stato, Polish Border Guard, Portuguese Immigration and Borders Services, Royal Netherlands Marechaussee, Slovenian Ministry of Interior, Spanish National Police, as well as experts from eu-LISA and JRC.

In addition, the European Border and Coast Guard Agency is grateful for the contributions of Agency staff from European Centre for Returns (ECRET), Centre of Excellence for Combatting Document Fraud (CED), Research and Innovation Unit (RIU), Risk Analysis Unit (RAU), Vulnerability Assessment Unit (VAU).

The European Border and Coast Guard Agency is also grateful to all those other stakeholders not mentioned here who contributed to the review process.

Executive summary

The mission of the European Border and Coast Guard Agency is to support the European Union in the application of measures relating to the management of the external borders by reinforcing, assessing and coordinating the actions of Member States (MS) in the implementation of those measures.

Research and Innovation represents one of the fields of activities of the European Border and Coast Guard Agency, as defined by Regulation (EU) 2019/1896. To fulfil its mission in this context, the Agency proactively monitors and contributes to the development of research and innovation relevant to European integrated border management, which serves as a platform to bring together Europe's border-control personnel and the world of research and industry to bridge the gap between technological advancement and the needs of border control authorities.

In addition, the European Border and Coast Guard Agency plays an active role in driving the process of harmonisation and development of best practices, technical guides and standards in border control, in line with existing and future EU measures.

The Entry/Exit System (EES) established by the European Union is expected, at the time of writing, to be fully operational in all MS by May 2022. MS are currently making preparatory arrangements in order to conduct tests and pilots throughout 2021. The implementation MUST be harmonised across all MS and equipment used at border crossing points has to meet minimum requirements to be operationally suitable for the introduction of the EES. In this context, the European Border and Coast Guard Agency is expected to support the MS in their preparation for the implementation of the EES in setting technical guide for equipment used for border checks.

The following methodological approach was adopted in drafting this technical guide: a Technical Expert Group (TEG) on EES equipment was set up by the Agency's Research and Innovation Unit (RIU) comprising MS, eu-LISA, and Joint Research Centre (JRC) experts specialising in EES border control solutions. In a series of meetings, the experts documented and assessed national practices and shared experience in the areas of interest, to provide a basis for the drafting of the technical requirements. The two main factors guiding the development of these requirements were that they:

- MUST be aligned with the MS technical and operational needs;
- MUST constitute a baseline (or minimum threshold), rather than the ideal.

The technical guide reflects the outcomes identified and agreed on by the TEG and the harmonised definitions of categories and classifications, which serve as the conceptual framework and the basis for determining the main functions needed by EES equipment.

In view of the European Border and Coast Guard Agency's mandate to support of MS procurements pertinent to the implementation of the EES, this technical guide provides an overview of the minimum requirements for Manual Border Control (MBC); Self-Service Systems (SSS); e-Gates & Automated Border Control (ABC) Systems; Mobile Systems.

This technical guide for Border Checks on EES related equipment provides MS with a baseline for interoperability and technical compatibility of the equipment used in different operational scenarios.

1. Introduction

1.1. Background

In 2019, over 115 million Third Country Nationals (TCNs) travelled to the European Union. By 2025, the number of TCNs is expected to rise to 176 million.

In response to these challenges, the EU decided to establish a new system for registering information on the entry, exit and refusal of entry of TCNs crossing the external borders of the MS.

Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES) was adopted in November 2017 and sets the boundaries for the future border control procedures at all external borders of the Schengen Area, including an amendment of the Schengen Borders Code (SBC).3

The system will apply to all TCN travellers who seek entry into the Schengen area for a short stay (a maximum of 90 days in any 180-day period):

- TCN Visa holder travellers;
- TCN Visa exempt travellers;
- Family members of EU nationals/TCNs enjoying the right of free movement without a residence card.

The EES Regulation does not apply to EU citizens, TCNs with a residence permit and family members of EU nationals with a residence card.4

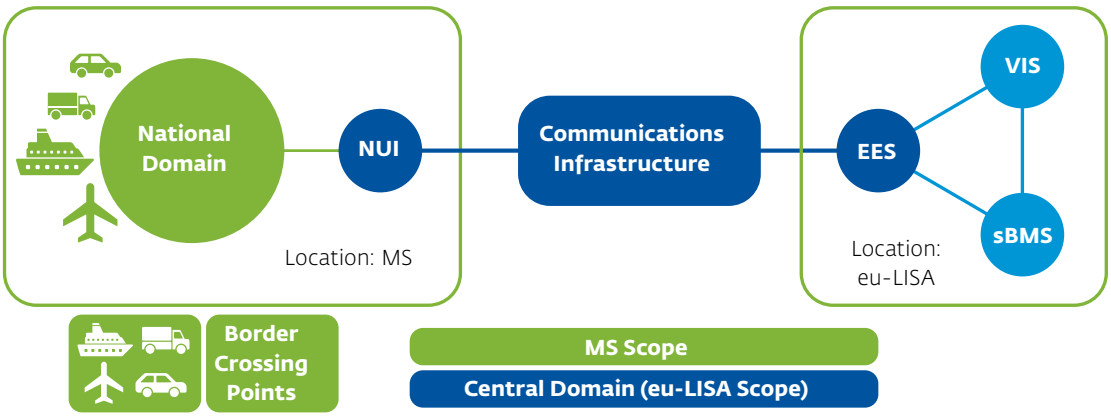

Figure 1: High level overview of EES Architecture and responsibilities

3 EU 2016/399 and EU 2017/2225.

4 For further details on which travellers the EES does not apply to, please refer to EU 2017/2226 Article 2(3) (a)-(h).

In particular, the border crossing processes will enrol biometric data (facial image and fingerprints, depending on the type of traveller) of the individuals within the EES Central System (CS-EES) for biometric verification at a later date, and a set of questions to be asked during each border crossing by this person. The system does not provide any provisions for storing the answers to the questions posed for verification of the entry conditions, and will also include an automated calculator for indicating the maximum length of authorised stay.

This will facilitate the detection of overstayers and support the identification of undocumented persons in the Schengen area or TCNs committing identity fraud or carrying false documents. The EES will also record refusals of entry.

The EES offers MS the ability to automate most of the data and information, capturing steps currently undertaken manually, and will replace the manual stamping of passports. The EES will be interconnected with the Visa Information System (VIS) and future ETIAS by a communication channel and be used by border control and consular authorities, allowing other services to be provided with interoperability including European search portal and multiple identity detection.

The EES enrolment or verification will trigger a check in ETIAS or VIS, and in the future will also find multiple identities in other EU information systems through the Shared Biometric Matching Service (sBMS).

The EES processes will potentially extend the time it will take to process a majority of TCNs at the external Schengen Borders. The concept behind using the SSS and ABC is to trigger all mandatory checks in the security databases (national, SIS, SLTD, etc.) as early in the process as possible, so that by the time the traveller is guided towards a border control booth or an e-Gate, all information will have reached the responsible border guard to help with the risk assessment of the traveller.

In addition, the EES will allow law enforcement authorities to perform certain queries for the prevention, detection and investigation of terrorism and other criminal offences.

Five types of scenario which can be used for the EES:

Manual Border Control (MBC): manual checks performed by border guards, e.g. at a specific border control station, which can be a fixed counter or a mobile/portable solution.

Self-Service System (SSS): a self-service station (e.g. a kiosk), located before Manual Border Control (MBC) or e-Gates, for pre-enrolment of the traveller's data. This allows the traveller to capture all necessary data (passport and biometrics) themselves and have their identity verified. The verification after pre-enrolment has to be processed by a border guard.

e-Gate: a physical barrier at a Border Crossing Point (BCP), operated by electronic means, that allows the traveller to pass through the border in a specific area, e.g. the airport terminal from airside to landside (Entry) or vice versa from landside to airside (Exit). An e-Gate and an SSS can make up an Automated Border Control (ABC) system.

Automated Border Control (ABC): an automated system which authenticates the e-MRTD, establishes that the passenger is the rightful holder of the document, queries border control records and automatically determines eligibility for border crossing according to pre-defined rules. There are different typologies of ABC; in particular, 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 entire transaction in a single process without the need to move to another stage. In an ABC system designed as an "*Integrated Two-Step Process*" the traveller initiates the verification of the document and of his/her eligibility to use the system at the first stage, and then if successful moves to a second stage, where a biometric match and other applicable checks are carried out. In an ABC system designed as a "*Segregated Two-Step Process*" the process of traveller verification and of passage through the border control are completely separated. The traveller verifies at the first stage, a tactical biometric is captured or a token is issued, and then the traveller proceeds to the second stage, where the tactical biometric or token is checked to allow exit. This typically takes the form of an SSS for verification of the document and the holder, while border passage occurs at an e-Gate. More details can be found in FRONTEX 2015.

These approaches support a fully automated border crossing process in terms of the contact between traveller and border guard, but do not mean that the mandatory decision making process or supervision challenges to mitigate against fraud can be ignored.

Mobile Systems: involving Temporarily Stationary Equipment, to be used at a BCP (or at cruise ships), which could be a suitcase version of a Manual Border Control (MBC) solution or a Mobile SSS; Portable Mobile Equipment that is hand carried by border guards or equipment carried by law enforcement personnel; and a Digital Mobile approach based on equipment such as a smartphone that is provided by travellers themselves and an application for travellers.

The Manual Border Control (MBC) process for the enrolment of the first border crossing of a TCN in the EES is RECOMMENDED to support the manual verification of the captured data, following the interpretation note issued by the Commission on 13 July 2020, has to be carried out by border guards using automated systems. This implies that a facial image and fingerprint need to be taken again at the time of the border checks, and a technical comparison of two images (not a visual check) needs to be included in the process.

For some border crossings under conditions explained below (see 3.3) at exit, the use of an ABC system MAY be allowed instead of the use of MBC, but the traveller MUST be carrying an electronic Machine Readable Travel Document (e-MRTD). For all deployments involving SSS and e-Gates, it is RECOMMENDED to adopt strong anti-fraud and risk mitigation measures.

This document describe the main common scenarios, the Handbook on EES will provide additional operational clarifications, not available at the time of developing this technical guide, to allow Member States to design their own alternative processes.

1.2. Purpose and audience

The EES entry into operation is expected in May 2022, driving the need for a change of border control processes and the deployment of new border control equipment at all BCPs (land, sea and air) throughout the Schengen Area and its external borders.

This technical guide addresses the demand from MS for flexible and timely support as they prepare for the entry into operation of the EES. It has been prepared so that national entities can apply the information it contains for their own purposes. The present document is therefore primarily intended for MS border management authorities, particularly technical and operational experts involved in the implementation of the EES at the EU's external borders; as well as the national procurement services involved in the purchase of equipment for these authorities. The document will be publicly accessible.

This technical guide may also serve as a reference document for the European Commission when deciding on the allocation of Internal Security Funds for the purchase of border control equipment, thus encouraging the purchasing of EU-compatible and inter-operable technical equipment through a harmonised set of minimum technical and operational requirements.

1.3. Scope and limitations

The European Border and Coast Guard Agency has set up TEGs consisting of experts from MS and European institutions, tasked to develop guidance on a set of technical requirements for various kinds of border control equipment. This technical guide is the result of that effort.

The Technical Guide drafted by the expert participating in the TEG is a consensus document developed as the output of workshops, with selected external experts from 10 MS who were engaged at the time of writing in the implementation of the EES at the national level, eu-LISA, JRC and the European Border and Coast Guard Agency, followed by consolidation of all the contributions into a unified draft and then consultations with all MS on the draft to ensure transparency. They are produced quickly to address the current needs of MS in areas where such guidance does not exist yet. This Technical Guide, which is non-binding, does not have the impact of more formal technical standards, but still possess an authority derived from the openness of the participation and agreement of the experts.

This Technical Guide may be further developed into more formal technical standards once a methodology has been developed with MSs. The common methodology will detail the management process for the development of the technical standards and define their reach for the various stakeholders.

The Technical Guide is therefore not assigned the status of a European Standard (EN) and there is no obligation for MS to withdraw pre-existing national standards which conflict with this document.

This Technical Guide for border checks on Entry/Exit System (EES) equipment addresses the technical, operational and performance requirements at all BCPs for the processes under which border checks can be carried out:

- Manual Border Control (MBC);
- Self-Service Systems (SSS);
- Automated Border Control (ABC) and e-Gates;
- Mobile Systems.

The present document does not address: (1) the requirements of consular posts responsible for the capture and processing of data during the application for and issuing of a visa prior to entry to the Schengen Area; (2) the requirements of the Schengen Borders Code, which still allows MS to use Self-Service Systems (SSS), e-Gates, or both, for border crossings by European Union citizens, as well as EEA and Swiss citizens, whose border crossing is not subject to an enrolment in the EES; (3) the technical solution to check their data in the EES, (4) any specific requirements for ETIAS, although the technical requirements of the equipment may also meet any national requirements.

1.4. Methodology and organisation of work

The conditions for the development phase of this Technical Guide were left deliberately light to facilitate its elaboration. They consisted of a series of workshops with selected external experts from 10 MS who were engaged at the time of writing in the implementation of the EES at the national level, eu-LISA, the JRC and the European Border and Coast Guard Agency, followed by consolidation of all the contributions into a unified draft and then consultations with all MS on the draft to ensure transparency.

Experts from Bulgaria, Czechia, France, Germany, Italy, the Netherlands, Poland, Portugal, Slovenia and Spain responded to the Agency's invitation. National experts were joined by experts from eu-LISA to provide insight and direction based on the parallel work and various activities of eu-LISA and other Working Groups, to support the timely entry into operation of the EES. In addition, experts from the European Border and Coast Guard Agency contributed to the organisation and the development of the final agreement.

A total of three workshops was held with the experts, to gradually gather contributions from MS. The first workshop resulted in an initial agreement on the document structure, based on an initial proposal by the Agency, and a distribution of experts among various sub-groups responsible for identifying the initial material for the development of the technical guide. On this occasion, MS experts also presented the national solutions being envisaged and the issues that arose. The material compiled by the experts could be consulted by the group members through a document-sharing platform set up by the Agency.

A second workshop was held to review the material and fine-tune the structure of the document. The sections of the document lacking any initial contributions were identified, and responsibilities to collect further material were assigned.

A third workshop was set up to review the contributions, resolve redundancies and discrepancies, and agree on the planning to complete this phase of gathering of technical contributions through exchange of materials on the platform and discussions in sub-groups.

The technical contributions were then consolidated and organised in a unified draft. This consolidation phase was carried out by the RIU. The consolidation process was closely followed, commented on and improved by the experts, by maintaining constant contact through e-mail and video-conference in small groups.

The draft was shared within the Agency through the Operational Board and again with all members of the TEG. Comments were also sought from all MS through the National Frontex Point of Contacts Network, to obtain comments from all national business units identified at the national level which would be impacted by the document. Similarly the draft was sent to the participants of the ETIAS/EES Advisory Group and to the Commission for comments. All comments were taken into account and the Agency kept a registry of comments received and their integration into the document, or the justification for not retaining these comments.

A plenary meeting was held with those stakeholders who expressed an interest in the final review and consolidation of the comments.

The consultation stage was considered complete once the Agency believed consensus had been reached among the technical experts and national business units on the content of the draft. This succession of consultations with MS means that the European Border and Coast Guard Agency has confidence that the document reflects a broad consensus among MS, the Agency, eu-LISA, the JRC and the Commission.

1.5. Harmonised definitions of categories and classifications

This document introduces all the concepts needed for a successful deployment of various BCP solutions located in the National domain (please see Figure 1) to address the data capture requirements for the EES and SHOULD harmonise workflows and approaches for:

- Manual Border Control (MBC);
- Self-Service Systems (SSS);
- Automated Border Control (ABC) and e-Gates;
- Mobile Systems.

To support this aim, the document is organised as follows:

- Chapter 2 addresses common technical, performance and other requirements for any of the BCP solutions identified above:
  - Types of travellers;
  - Travel document reading and authentication;
  - Facial capture and capture system requirements;
  - Fingerprint capture and equipment requirements;

- Data quality;
- Traveller requirements;
- Logging;
- Health and safety;
- Vulnerability assessment, security and testing;
- Training.

- Chapter 3 addresses general and operational requirements for each of the BCP types identified above:
  - Manual Border Control (MBC);
  - Self-Service Systems (SSS);
  - Automated Border Control (ABC) and e-Gates;
  - Mobile Systems.

- Chapter 4 lists all the relevant references — European, international and national (where they exist) — to allow readers to find the original text which the recommendations contained in the document are based on.

- Chapter 5 has a list of common definitions.

The overall workflow between MS systems (BCPs and MS Central Systems located in the National domain) and the CS-EES via the National Uniform Interface (NUI) and the workflow within the Central System are not addressed in this document and can be found in relevant EU legislation detailed in Chapter 4.1. Performance indicators (availability and operational response targets) for the CS-EES are presented in C(2019) 1260. The connection between the Central domain and the MS domain will be implemented according to the specifications detailed in the Interface Control Document (ICD) elaborated by the EES-ETIAS AG (EL-ICD). The connectivity of the EES will be guaranteed by eu-LISA from the Central domain to the NUI, and by individual MS from the NUI to the BCP in compliance with the EES-ETIAS AG ruling on the data centre preparation for MS (EL-DCP) and Article 43 of the EES Regulation on business continuity and disaster recovery plan.

1.5.1. Manual Border Control (MBC)

The aim is to address the technical and operational requirements for Manual Border Control (MBC), to enable MS authorities to understand the processes of border control in the context of various pre-enrolment and other scenarios:

- Did travellers use the SSS before arriving at the MBC?
- What is the process for TCN visa holders?
- What is the process for visa exempt TCNs?

MBC will be the only configuration of BCP which MUST process TCNs carrying non e-MRTDs. The border guard SHALL assess the results of the launched traveller data (alphanumeric and biometric) searches delivered as candidate lists by the various national systems and the CS-EES. When hits are identified, the border guard SHALL have the option of sending the traveller to the Second Line at any time in the process or link existing records with those of the traveller. The border guard SHALL acquire the missing biometrics or assess the quality of the biometrics acquired previously and SHALL recapture them if necessary.

In addition, the border guard SHALL have the option to restart the border control process at any time in the process. If the enrolment process indicates fraud, the data SHOULD NOT be discarded but kept and used as evidence. However the fraudulent data SHALL NOT be entered into the EES.

1.5.2. Definition of systems: SSS, e-Gate, ABC

Definitions as per EU 2017/2225, which amends the SBC defined under EU 2016/399.

Self-Service System (SSS)

ⓘ an automated system which performs all or some of the border checks that are applicable to a person and which may be used for pre-enrolment and enrolment of data in the EES

The aim is to address the general and operational requirements for the SSS to enable MS authorities to understand the challenges of deploying such systems and what other elements need to be considered to ensure an optimal and anti-fraud approach:

- How can optimal data quality capture be ensured under different environmental conditions (e.g. lighting);
- What is the number of SSS per Manual Border Control (MBC) station;
- Can SSS deployments be redeployed elsewhere or used to support additional/ alternative processes;
- What supervision and monitoring are required;
- What logging is required;
- What evaluation of the deployed system is required.

An SSS MUST be used only by TCNs carrying an e-MRTD. The facial image of the traveller is acquired and verified against the reference facial image stored in the e-MRTD. Additionally, it is RECOMMENDED to compare the DG2 reference image and the cropped image scanned from the biographical data page. Any traveller without an e-MRTD trying to use an SSS MUST be directed immediately to MBC. For TCN visa holders, the capture of the fingerprints MAY be started in parallel with the verification process of the captured facial image.

All captured data is sent to the CS-EES to launch an automatic centralised identification process as well as a verification of fingerprints against the CS-EES (sBMS) if appropriate. In addition, for some use cases an identification process with fingerprints in VIS is started. Note that during the process of receiving the identification results the traveller SHALL never be stopped from proceeding to the next step in the border control process.

Note further that for some use cases, the identification process in the CS-EES and VIS is only launched based on the outcome of prior verifications in the respective systems, e.g. if a TCN has replaced their original MRTD.

e-Gates and Automated Border Control (ABC) Systems

ⓘ e-Gate means infrastructure operated by electronic means where an external border, or an internal border where controls have not yet been lifted, is actually crossed

ⓘ Automated Border Control (ABC) system means a system which allows for an automated border crossing, and which is composed of a self-service system (SSS) and an e-gate

The aim is to address the general and operational requirements for ABC to enable MS authorities to understand the challenges of deploying such systems, and what other elements need to be considered to ensure an optimal and anti-fraud approach:

- What is the number of e-Gates per SSS/MBC;
- What are the requirements for mantrap e-Gate solutions versus single door e-Gate solutions;
- How to decide about access, e.g. can all travellers enter a mantrap, or just specific groups of travellers;
- What evaluation of the deployed system is required.

An ABC system MUST only be used by a TCN carrying an e-MRTD. The facial image of the traveller is acquired and verified against the reference facial image stored in the e-MRTD. Any traveller without an e-MRTD trying to use an ABC MUST be directed immediately to a MBC.

1.5.3. Mobile Systems

The aim is to address the technical and operational requirements for solutions which are mobile to enable MS authorities to understand the challenges of deploying such systems:

Mobile Systems can be divided into three categories:

- Temporary Stationary Equipment
  Equipment that can be moved to a location temporarily to be used for a certain period of time, such as mobile kiosks (Mobile SSS) or portable (suitcase) for MBC stations that are established due to the specific requirements/location of the individual BCP, e.g. BCPs where TCNs only arrive occasionally (e.g. one flight/cruise ship per week).

- Portable Mobile Equipment
  Equipment that is hand carried by border guards, supporting smartphone-like solutions. These solutions can help address travel peaks or handle border crossings at remote or "difficult" BCPs. The requirements also address solutions used by police forces within the Schengen Area e.g. to check people against the EES/VIS.

- Digital Mobile equipment and application for travellers
  A solution based on equipment such as a smartphone that is provided by travellers themselves to perform certain steps of the border control procedure, such as answer a questionnaire at home or on an airplane, prior to arrival at the BCP, and provide a QR-code to SSS/ABC/MBC, etc.

2. General technical and performance requirements for EES

The following section presents the general requirements and processes for the EES, which are needed for all their components: Manual Border Control (MBC), Self-Service Systems (SSS), e-Gates, Automated Border Control (ABC) Systems, and Mobile Systems. Specific requirements for the components are presented in Section 3.

2.1. Types of travellers

Traveller type is determined by the National Border Management System. This is used to determine whether the TCN is registered in a National Facilitation Programme (NFP), is a Freedom of Movement Traveller (FOM) or holds a Residence Permit (RP) of that MS.

It is at the discretion of MS to define various TCN traveller categories, in accordance with Regulation (EU) 2017/2226 art. 2.

This document does not specifically address any special needs of the Reduced Mobility Traveller (RMT), however it assumes that MS will put in place solutions which can be easily accessed and used by RMTs and which address a full range of disabilities: in particular hearing, sight and mobility. Note that at a specific BCP, not all types of components might be present or that not all types of components present might be available in a special needs version.

2.2. Travel documents

Machine Readable Travel Documents (MRTDs) are official documents, conforming to the specifications contained in ICAO 9303, which contain mandatory visual data (VIZ) and a separate mandatory data summary in a harmonised machine readable format (MRZ). In addition to this data, e-MRTDs (which represent about 90% of all MRTDs in circulation in the world) carry an embedded contactless integrated circuit that offers the capability of being used for biometric identification of the document holder in accordance with ICAO 9303 standards.

Within the context of the EES:

- It is MANDATORY for all Non e-MRTDs to be processed through an MBC. An SSS MAY be used for pre-acquisition of data from travellers using Non e-MRTDs, provided that this data is not sent to the EES but stored temporarily for the conclusion of border control at the MBC;
- All MRTDs MUST have a validity of at least 3 months after the intended date of departure of the traveller from the Schengen Area (EU 2016/399);
- The MRTD MUST have been issued in the last 10 years (EU 2016/399).

2.2.1. General requirements for document authentication

Dedicated scanning equipment provides support to recognise and evaluate the features of MRTDs, especially optical/physical properties. These properties are intended as an additional indicator of the authenticity of the document. The integrated chip of an e-MRTD contains the digital information that is printed or engraved on the Visual Inspection Zone (VIZ) of the document, e.g. name, date of birth, place of birth, but also biometric data of the holder (minimum is a digital copy of the facial image) and cryptographic data that ensures that a given document was issued by an official entity and was not altered, cloned (if the chip supports AA or CA) or forged.

The main characteristics of travel document authentication are:

- Authenticity: check that the document is genuine, originating from the issuer;
- Integrity: check that the document data has not been altered, is not counterfeit or false; and
- Validity: check that the document has not expired, has not been reported as lost or stolen, and is not a fantasy document.

REQUIRED checks on MRTDs are as follows:

- Optical checks:

Optical inspection checks are made on physical security features placed on a given document type (e. g. special print design properties, brightening agents' free substrate, holograms etc.). Refer to Section 2.2.3 for further information.

- Electronic checks on e-MRTDs:

The electronic features of the RFID-chip are read and validated (e. g. access control, integrity of data and authenticity of chips). Refer to Section 2.2.3 for further information.

- Combined checks on e-MRTDs:

These checks perform a comparison of the data on the basis of the preceding two checks (Refer to Section 2.2.3 for further information) such as:

- comparing the optically read MRZ from the passport's page with DG1 stored in the chip;
- comparing biographic data from the data page (VIZ) with MRZ and/or DG1;
- matching the facial image on the data page with the facial image stored on the chip (DG2).

Other checks SHOULD also be performed, for example:

- Biometric checks:

For all MRTDs, it is RECOMMENDED to compare the facial image on the VIZ against the live captured facial.

For e-MRTDs, compare the live face of the document holder (traveller) against the facial image stored in the e-MRTD initially stored when the travel document was created and against the facial image on the VIZ. The captured live biometric data verifies that the current document holder is the same person the document was issued to.

- Background system checks:
  - Automated requests to background information systems on the basis of the information featured on an MRTD (e. g. checking data printed on the MRZ or from DG1 with official databases such as SIS, INTERPOL etc.). Note that the check in SIS SHOULD also be performed biometrically.
  - Automated optical checks against a Travel Document Patterns Database. Such databases MUST be kept up to date to avoid significant increases in the False Reject Rate (FRR).

2.2.2. Requirements for document readers

The document reader SHALL:

- Have a scanning surface large enough to handle all MRTDs (according to ICAO 9303):
  - TD-1, TD-2, and TD-3 for travel documents as well as MRV-A, and MRV-B for visas;
- Capture images of the travel document under near-infrared light (in the B900 band, cf. document specification according to ISO 1831), under UV light of a wavelength of approx. 365 nm and under white light reflecting colours of the visible spectrum in roughly equal amounts. These images SHALL be provided in PNG or JPEG format with an image resolution of at least 385 ppi (600 ppi is RECOMMENDED);
- Detect the presence of a document. The detection process SHALL still be carried out optically, even if an expected chip is absent or malfunctioning. The equipment and software SHALL be able to compensate for potential rotation and realign the image automatically and SHALL crop the captured data page accordingly for further processing;
- Read the MRZ automatically after the complete personal data page has been placed on the capture surface;
- Read e-MRTDs with an electrically conductive shielding;
- Read the personalized data page optically without any interference;
- Capture an image of the travel document in visible wavelengths (refer to ISO 1831);
- Have maximum reading time for 99% of all documents of:
  - 5 seconds until MRZ is present;
  - another 7 seconds until the document has been read completely electronically.

Also, the document reader SHOULD be able to:

- Read the six-digit Card Access Number (CAN) that can be found on some e-MRTDs (either in the MRZ or in the VIZ). If CAN is available, use CAN for Password Authenticated Connection Establishment (PACE);
- Electronically read an e-MRTD with integrated metal protection foil (e.g. USA passports) without interruption;

- Read electronic documents where the chip is not integrated in the photo data page (but is located in the front or back cover, for example).

Also the document reader SHOULD be integrated with a Travel Document Patterns Database that is regularly updated (minimum every 3 month).

- The software MUST be able to be adapted as needed to changes in documents (subsequent correction, extension and readjustment to take into account findings from real documents, for example ageing artefacts, traces of use, production fluctuations).

2.2.3. Workflow for document authentication

Document authentication is MANDATORY at BCPs.

The process (please see Figure 2) starts with reading the optical/physical features of an MRTD. Depending on the operational scenario, the optical images of the data page and the MRZ or the CAN are read. Based on this data, a logical check (e.g. checking the validity of the document is MANDATORY) as well as a check of the optical/physical security features of the document are performed followed by a RECOMMENDED verification of the security patterns (UV, IR, Visible) using a database for pattern check provided by specific document scanner SDK vendor. Reading the document electronically can start as soon as the MRZ and/or the CAN of the document are available and an RF chip is identified. Combined optical and electronic checks SHALL be performed as soon as the optical and electronic data required for such checks are available.

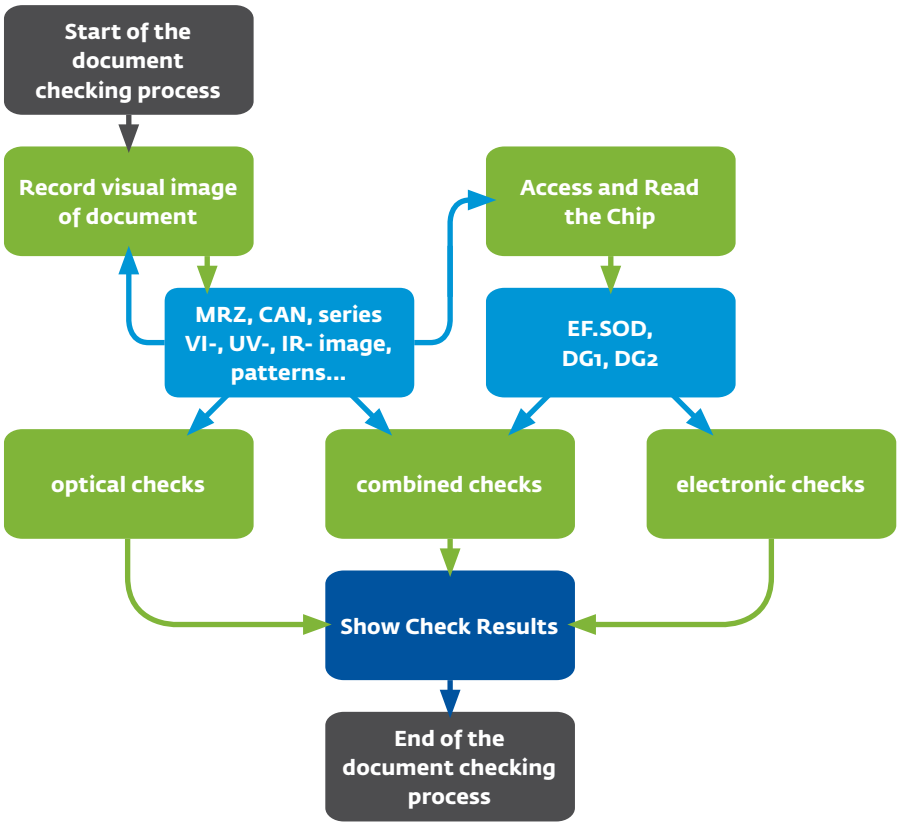

Figure 2: Workflow for checking e-MRTDs

Optical Checks on Travel Documents
The following optical document checks SHALL be performed to ICAO 9303:

- Check document model, refer to Best Practice Guidelines for Optical Machine Authentication, Part 1, Version 1.2, International Civil Aviation Organization (ICAO), 2018;
- Spectrally selective checks, different reactions occurring on a document illuminated with visual (VI, white light) or with extra-visual (UV, IR) illumination, refer to BSI-TR03135 and ICAO 9303;
- Check MRZ for ICAO 9303 compliance;
- Check the MRZ's consistency;
- Check MRZ is readable under IR light;
- Check MRZ is printed using OCR-B type face, refer to ISO/IEC 30116.

Electronic Checks on Travel Documents
To check the electronic components and digital security features of e-MRTDs, standardised protocols and specifications SHALL be performed. These protocols are based on hierarchically structured public key infrastructures, confirming that the data stored on the electronic MRTD was not altered, is trustworthy and that a chip was not cloned. The process SHALL involve:

- Elementary File with Security features (EF.SOD) verification;
- DS Certificate signature verification;
- Certificate validate period check;
- DS certificate revocation status;
- Comparison between EF.SOD and EF.COM;
- Data group integrity check;
- Issuing country comparison (DG1 vs DS Certificate).

For a complete electronic check, an Inspection System SHALL support:

- Master Lists management and verification of Document Signer (DS) and Country Signing Certification Authority (CSCA) certificates;
- DS List management;
- Defect Lists management for a given DS or CSCA certificate;
- Various security mechanisms and standards enforced by C (2018) 7774:
  - Basic Access Control (BAC) as defined by ICAO 9303;
  - Password Authenticated Connection Establishment (PACE) as defined by ICAO 9303 and BSI-TR03110;
  - Passive Authentication (PA) as defined by ICAO 9303;
  - Active Authentication (AA) as defined by ICAO 9303;
  - Chip Authentication (CA) as defined by ICAO 9303;
  - Terminal Authentication (TA) as defined by BSI-TR03110.

More details about the verification of e-MRTD chip data can be found in FRONTEX 2015, section 4.1. An example of detailed requirements for the process of e-MRTD authentication and a comprehensive description of the procedures that comprise a full featured e-MRTD inspection can be found in BSI-TR03135, part 1, section 4.

Combined Checks of Travel Documents
The following combined checks SHALL be performed:

- Issuing country comparison (DG1 versus DS certificate);
- Check the expiration date of the document, compare extracted date of expiration from travel document (data group 1) with the current date;
- Check the optical biographic data against the electronic biographic data;
- Checks across several documents:
  - Check an electronic MRTD's MRZ against the visa's MRZ;
  - Check an electronic MRTD's MRZ against the residence permit's MRZ;

In addition, it is RECOMMEND to perform:

- Comparison of the personalisation contents, compare data extracted from the MRZ with data extracted from the Visual Inspection Zone (VIZ) on the data page;
- Checks on both sides of an ID-1 sized electronic MRTD;
- Check DG2 against the facial image from the VIZ, compare the electronically stored facial image with the facial image from the VIZ;

Defects in Travel Documents
During the production of MRTDs errors may occur, both in the optical/physical parts of the document and in the electronic components, and a personalisation error could affect a large number of MRTDs (e.g. the set of e-MRTDs based on one particular DS certificate). The withdrawal of an issued e-MRTD affected by a defect is generally impractical or even impossible especially if the defect relates to foreign e-MRTDs.

Defect Lists define such errors, and not only inform border personnel about erroneous MRTDs but also provide corrigenda to fix the errors or procedures for processing a traveller carrying such a document where possible. Regular DS certificate revocation information (e.g. from CRLs) can also be included into such Defect Lists.

It is RECOMMENDED always to use such Defect information about erroneous e-MRTDs during the process of document authentication. In particular for SSS and ABC systems, the traveller MUST be directed to an MBC for further checking to prevent the processing of a fraudulent document, and the system SHALL report an error when a defect occurs.

2.3. Biometric capture and verification

EU 2017/2226 states:

- Four fingerprints per visa-exempt TCN SHALL be registered in the EES, if physically possible, to allow for accurate verification and identification, thus ensuring that the TCN is not already registered under another identity or with another travel document:
  - Travellers under the age of 12 no fingerprints are captured;
- The fingerprints of visa-holding TCNs SHALL be used if the TCN is not yet registered in the EES.
- The facial image of both visa-exempt and visa holding TCNs SHALL be registered in the EES.

Fingerprints or facial images SHALL be used as a biometric identifier for verifying the identity of TCNs who have been previously registered in the EES.

Please refer to EU 2019/329 for the quality, resolution and use of fingerprint and facial images for biometric verification and identification in the EES. Note that the target value for the Failure To Enrol Rate (FTER) is zero. Member States SHALL take care to avoid such cases by using a quality-focused enrolment process.

2.3.1. Requirements for facial images

Facial Image Quality
The quality parameters for live captured facial images are as follows:

- For captured facial images the image requirements of ISO/IEC 19794-5:2011 SHALL be met:
  - Frontal facial images SHALL be captured;
  - The colour depth SHALL be 24 bit RGB or 8 bit grey scale;
  - The minimum distance between the eyes (inter-eye distance) for capture positions of the traveller SHALL be at least 120 pixels (EU 2019/329), preferably 240 pixels (ISO/IEC 19794-5:2011);
    - OPTIONAL for e-Gate scenarios, a lower inter eye distance MAY be used (e.g. if the traveller is moving through the e-Gate) for the capture process (RECOMMENDED no less than 80 pixels) in a verification workflow.
  - Dimensions of the captured images SHALL be:
    - Image width = 600 pixels maximum 1,200 pixels
    - Image height = 800 pixels maximum 1,600 pixels
  - The face SHALL be fully visible in the foreground of the captured image so that the face takes up most of the image area - multiple faces SHOULD NOT be visible. The face SHOULD be cropped (using a tight frame, see figure 3) and de-rotated from the overall scene in the captured image.

The quality of the captured facial image SHALL be assessed, following the criteria stated in ISO/IEC 19794-5:2011, during the capture process at the national level by MS at the time of capture prior to its transmission to the CS-EES. A quality assessment tool (USK) will be made accessible by eu-LISA and MAY be used (actually strongly advised to be used) if data are submitted to the Central System.

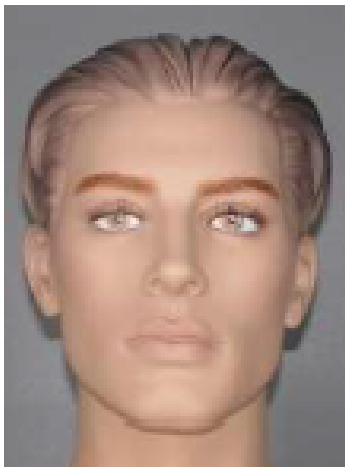

Figure 3: Example of tight framing around the face

- OPTIONAL, if no facial image can be captured, the digital facial image from DG2 of an e-MRTD MAY be sent to the CS-EES. Note that the DG2 SHALL NOT be enrolled without the electronic verification of the travel document and that this DG2 image SHALL be updated as soon as possible;
- Note that a uniform background, as mentioned in ISO 19794-5:2011, is not mandatory for border control components.

The ability to capture the facial image of any traveller SHALL be integrated into all border control components:

- Manual Border Control (MBC);
- Self-Service Systems (SSS);
- e-Gates and Automated Border Control (ABC);
- Mobile Systems.

However it is recognised that different facial capture solutions are needed for each component. Details on the specific requirements of each component are contained in the relevant subsection in Section 3.

Presentation Attack Detection on Facial Images

For unsupervised components, the capture process SHALL contain a presentation attack detection (PAD) subsystem, detecting spoofing attempts where an attacker tries to establish a different facial image as a probe image in the verification or identification process. Supervised components SHOULD contain such a PAD subsystem. The PAD MAY consist of hardware and software (e.g. the facial capture system MAY have additional sensors designed for this purpose).

Well-known attacks, which SHOULD be detectable by the facial capture solution, are:

- Photographs printed on paper or textiles (T-shirts);
- Photographs displayed on electronic devices (e.g. phones, tablets, laptops);

- Videos displayed on electronic devices, especially showing motion of the biometric subject;
- 3D masks (paper-based or other materials).

PAD performance SHOULD be assessed through Common Criteria. Also, please see ISO/IEC 30107-3:2017, which includes approaches for PAD testing. It is RECOMMENDED that PAD checks be performed during the biometric capture process.

The result of the PAD MUST be included in the logged data from the capture process.

Facial Capture System

The facial image capture system will be composed of at least the following elements:

- Image capture elements (camera, video or still, or combination of cameras working together) SHALL be capable of capturing high quality non-blurred images at a resolution to meet ISO 19794-5:2011 within the designated capture area:
  - SHALL NOT require the user to change position in front of any camera;
  - SHALL include automatic focus;
  - SHALL include adjustable depth of field;
  - SHALL include video camera capture frequency of at least 8 frames per second in automated mode;
  - OPTIONAL independent power;
  - Image capture elements SHALL allow usage at least at the following conditions: 0-40° C, 10-90% humidity;
  - SHALL include standard high-speed connection and interface.
- Lighting elements (hardware or software) to address the environmental challenges of capturing a face that is illuminated evenly:
  - Automatic adjustment of gain (contract and brightness);
  - Usable in low lighting environment;
  - Able to capture even and shadow-free illuminated facial images;
  - Automatically controlled continuous illumination (no flash) and diffuse;
  - Mirroring effects of glasses SHOULD be avoided.
- Pre-processing software (and optional hardware):
  - Lossy compressions of captured facial image data SHALL NOT be allowed;
  - The capture software of the camera system SHALL provide uncompressed image data for further processing. It SHALL either provide raw uncompressed image data or use a lossless image container format (JPEG, ISO IEC 10918, or JPEG2000, ISO/ IEC 15444:1, with maximum compression rate 1:20). The final format for images that are used with the EES Central System SHALL be JPEG or JPEG2000;
  - The maximum of the resulting file size of the image SHALL be 375 kB;
  - Integrated quality control assessment to meet EES requirements;
  - The system MAY measure the distance between the traveller and the image capture elements (the distance is measured from the forehead of the traveller to the active image capture system's optics).

Additionally, the capture system MAY have a screen or monitor facing the traveller which displays the image of the traveller being captured and which can help the traveller position themselves correctly in front of the cameras (digital mirror). Additional sensors MAY exist that support the image capture tasks such as:

- Independent photometers;
- IR sensors to detect the presence/height of the traveller, etc.

Facial Capture Process
The process SHALL use the following steps:

1. The biometric subject SHALL be guided to present his/her face;
2. Facial capture process SHALL be triggered automatically depending on the use case;

The camera system SHALL automatically adjust for the height of the traveller.

The angle between camera axis and axis of the traveller's face (pitch, roll and tilt) SHALL be within the range of-5 to +5 degrees to compare with a full frontal image if the traveller is in the designated capture area.

- Height range for travellers using SSS, e-Gates and ABC SHALL be at least 120 cm to 200 cm in height.

If there are multiple faces in the capture image area they SHALL be detected. Note, detection SHALL be carried out all the time during the capture process until the facial image is captured and accepted as being of a sufficient quality for comparison.

- If multiple faces are detected, user guidance SHALL inform the traveller to appear alone in front of the capture system.

The distance of the biometric subject to the facial capture system SHALL be determined by the type of component to be deployed:

- Manual Border Control (MBC);
- Self-Service System (SSS);
- e-Gates and Automated Border Control (ABC);
- Mobile Systems.

If the biometric subject is not in the optimal capture range, assisting personnel /border guard guidance SHALL guide the traveller into the optimal distance range.

If a facial image cannot be captured within a configured timeout, e.g. the biometric subject does not look at the camera or disappears from the system, the capture processes end. The timeout SHALL be configurable (by component or scenario).

The quality of the captured facial image SHALL be assessed. The assessment SHALL address at least the following criteria (refer also to ISO 19794-5:2011):

- Pose, expression and pitch, roll and tilt of the head;
- Illumination on the face, sufficiently and evenly lit;
- Position of the eyes and the number of pixels between them;
- Sharpness and resolution of the captured image.

If the quality is not sufficient and the timeout is not exceeded, a facial image is continuously captured until an image meets the quality requirements (see the chapter "Facial Image Quality"). The timer for the timeout SHALL start with the capture and assessment of the first facial image from the facial capture system. The timeout MAY vary by component.

If the quality is sufficient, the workflow proceeds to the next step.

If the timeout is exceeded and no image of sufficient quality is captured, the best facial image is selected from among all the images captured according to the Quality Assessment Tool (see the chapter "Facial Image Quality") and the workflow proceeds to the next step. If the image is submitted to the CS-EES, its quality has to be flagged.

With optimal conditions for a low risk traveller, the overall facial image capture process SHALL NOT exceed 10 seconds. Where the system is not required to perform a PAD (e.g. under supervised scenario of the MBC and Mobile Systems) the overall facial image capture process SHALL NOT exceed seven seconds.

All transactions submitted to the CS-EES SHALL meet JPG [(ISO/IEC 10918] or JPEG 2000 [ISO/IEC 15444-1] image compression standard. The maximum allowed image compression rate is 1:20.

Facial Performance Requirements
The following requirements MUST be met to ensure facial verification (1:1 comparison), performed by the EES Central System:

- Please see EU 2019/329 A, Paragraph 1.2.2, Accuracy of Biometric verification and Paragraph 1.2.3, Accuracy of biometric identification for:
  - The maximum values of FNMR and FMR.
  - The false negative identification rate (FNIR) and the false positive identification rate (FPIR).
- These thresholds SHALL be configurable at national level to allow for stricter settings when necessary.
- Please refer to ISO 19795 for all the necessary steps to plan, execute and report on biometric testing to check the validity of claims:
  - The provider of the facial verification solution MUST provide sample calibration data based on operational performance, to identify and remove the deterministic errors from the sensors based on MEMS (Micro-Electro-Mechanical Systems) technology.
  - To ensure the validity of declared values, a provider SHALL provide offline test results that support each claim. The following requirements apply to those test results:
    - Such performance SHALL be on the basis of images of comparable characteristics (e.g. images in size and resolution and pose variation of a typical e-MRTD deployment).
    - The provider SHALL provide as a minimum a DET curve and a graph showing the performance on the supplied operational data.

Testing and Evaluation of Facial Capture Systems
Test cases to assess facial capture systems in general:

- Performance (speed):
  - Assess the duration of image capturing on the basis of log files (see Section 2.7);
  - Ensure that captured images are within the specified time limit;
- Image quality under perfect environment conditions:
  - Assess quality of captured image;
  - Expert opinion;
  - Maximum diversity of test subjects (age, gender, height, etc.);
- Image quality under changing environment conditions:
  - Assess quality of captured image, expert opinion, maximum diversity of test subjects (age, gender, height, glasses etc.):
    - Changing levels of brightness;
    - Changing levels of colour temperature;
    - Changing light frequencies;
    - Changing backgrounds;
    - Changing angles of lighting.

Test cases to assess PAD of facial capture system:

- Artefacts:
  - Masks: silicon, latex, printed 3D masks;
  - Photos presented on displays: smartphones, tablets;
  - Printed photos: Paper, T-shirts, optical data page of MRTD;
- Present artefacts to camera.
  - Analyse percentage of cases (per artefact class) where the PAD component did not detect that an artefact was presented. If the camera is not taking any picture at all, the measurement SHOULD be noted as "component noticed artefact" (please see ISO/IEC 30107-3 for recommended metrics).
- Also, present low risk faces to the camera to avoid overfitting of PAD component to artefacts by providers, which often adds time to the overall process.

2.3.2. Requirements for fingerprint images

Fingerprint Image Quality
Quality thresholds for captured fingerprints are as follows:

- Enrolment
  - Version 2.0 (or newer) of the Fingerprint Image Quality (NFIQ) metric defined by NIST SHALL be used for verifying the quality of the captured fingerprint.
  - Quality assessment of the captured data MUST be performed prior to transmission to the CS EES. A quality assessment tool (USK) will be made accessible by eu-LISA and MAY be used (actually strongly advised to be used) if data are submitted to the Central System.
- Verification**:**
  - Version 2.0 (or newer) of the Fingerprint Image Quality (NFIQ) SHALL be used for verifying the quality of the captured fingerprint, or where technically impossible, by using another metric which SHOULD preferably be correlated with the NFIQ version 2.0 (or newer version).

Data Capture Requirements

Fingerprints SHALL be captured from all travellers during enrolment or during verification if necessary. Children under the age of 12 are to be excluded from this requirement. Note that this age limit may change in future versions of the EES Regulation. In this case, the new age limit applies here.

Travellers without fingers or without fingerprints are always excluded from the requirement of taking fingerprints, but as long as one fingerprint can be obtained, the right hand should be used. However, where the physical impossibility is of a temporary nature, that fact SHALL be recorded in the EES and the person SHALL be required to give fingerprints on exit or at the subsequent entry.

Within the standard process fingerprint data from the right hand (4 fingers flat, slap) SHALL be captured where present. Otherwise, the corresponding fingerprint data from the left hand (4 fingers flat, slap) SHALL be acquired.

In a supervised setting (such as MBC and Mobile Systems), if the traveller is not physically capable of placing all 4 fingers on the fingerprint scanner at the same time to achieve a good quality image, the border guard MAY capture each finger of the slap in single finger capture mode. This SHALL be possible during the entire process. If fingerprints are captured singly or on single finger readers e.g. on a Mobile System, a uniqueness check of all fingerprints captured MUST be performed.

The slap image SHALL be segmented into single fingerprints. For this segmentation process, the following requirements SHALL be fulfilled:

- Ability to accept rotated fingerprints in the same direction up to 45°;
- Rotated fingerprints in the same direction have to be corrected to be vertical;
- Segment the first part over the finger (fingertip);
- Segmentation has to occur on uncompressed data;
- The slap image SHOULD be checked for which hand it has come from (right or left). Depending on the component being used, if the assessment does not match what was requested, a message MUST be displayed for the user/operator to confirm the situation.

Presentation Attack Detection (PAD) SHALL be used in any unsupervised scenario (e.g. at the SSS). In a supervised setting, it is RECOMMENDED that PAD checks be performed during any capture process.

Fingerprint Image Quality

Each fingerprint SHALL be assessed regarding the quality of the capture. As the quality algorithm, NFIQ 2.0 SHALL be used. For plain fingerprints, the following NFIQ 2.0 minimum thresholds SHALL be met:

- index finger: 20
- middle finger: 20
- ring finger: 10
- little finger: 10.

A fingerprint image with compression algorithm WSQ (ISO/IEC 19794-4:2011 from 500 ppi) or JPEG 2000 (ISO/IEC 15444-1 from 1000 ppi) is MANDATORY for all transactions to the CS-EES.

If the quality requirements for one or more fingerprints of the slap are not met, the capture SHALL be repeated up to two times (i.e. the capture of a single slap consists of a maximum of three capture attempts).

If the quality check of the third capture attempt fails, the best of the captured slaps SHALL be identified and temporarily stored along with corresponding information.

A sequence check SHALL be conducted for the captured slap image to detect the capture of wrong fingers, e.g. due to interchanged hands or multiple captures of the same hand or finger. Additionally, a slap classifier SHALL be used for the captured slap image to detect the capture of the wrong slap. If the wrong slap has been captured, the traveller SHOULD be invited to have the slap recaptured.

Presentation Attack Detection on Fingerprint Images
For unsupervised components, the capture process SHALL contain a presentation attack detection (PAD) subsystem to detect spoofing attempts using artefacts by which an attacker tries to establish either different fingerprints or poor fingerprints as probe images in the verification or identification process. Supervised components SHOULD contain such a PAD subsystem.

The PAD system MAY consist of hardware and software (e.g. the fingerprint scanner MAY have additional sensors or software options designed for this purpose).

Typical artefacts consist of fake fingers made from materials such as, but not limited to:

- Modelling compound (e.g. Play-Doh), latex, Window Colour, white silicon, transparent silicon, candle wax, white glue, gelatine, foil, photocopy on paper, wood glue, Micro Kristal Klear, potato, graphite, etc.).

These materials are used to create fake fingers to test the spoof detection functionality. The presentation attack detection subsystem SHALL be able to detect all well-known attack types.

PAD performance SHOULD be assessed using Common Criteria. Also, please see ISO/IEC 30107-3:2017, which includes approaches to PAD testing.

Fingerprint Capture System
It is RECOMMENDED to use a four-finger scanner.

The fingerprint scanner MUST be easy to clean in order to minimize quality losses due to contamination and to ensure appropriate hygiene.

Fingerprint Capture Process
With optimal conditions for a low risk traveller, the overall finger slap capture process SHALL NOT exceed ten seconds.

Four fingers (index finger, middle finger, ring finger, little finger) of the right hand as the standard case, if available, SHALL be captured, otherwise the left hand.

The built-in fingerprint sensor SHOULD trigger automatically if the required fingers with the appropriate quality are detected or a configurable time has been exceeded.

To prevent unwanted duplicate acquisitions of the same fingers or slaps, the software SHOULD NOT start the capture process before the fingers from a previous capture have been removed from the sensor surface.

The fingerprint system SHALL take appropriate measurements to prevent unintentional mixing of the left and right hands, e.g. by structural measures such as positioning the system in a way that favours the usage of the right hand (for the standard process). In addition, the system MUST be able to distinguish right from left hands ("Slap Classifier").

The algorithmic classification SHALL have a performance level of at least 99% availability and its threshold SHALL be configurable.

It SHALL be configurable to switch the algorithmic classification off or to use the classification result information only for evaluation purposes.

The captured fingerprint data MUST be quality checked through a local tool quality assurance process or OPTIONALLY using the eu-LISA USK toolkit.

The images provided by the fingerprint capture software SHALL comply with the format for captured fingerprints as described in ISO/IEC 19794-4:2011 and with NIST2.0 (or newer) quality.

The capture process SHOULD prefer the highest quality image of a sequence, at least the last captured image (after time-out) of a sequence. This functionality MAY be part of the firmware and MAY NOT be available as a separate software component.

If the Acquisition Software allows multiple thresholds for pre-qualifications, the thresholds of the pre-qualification for performing a capture SHALL be documented by the provider and be configurable by the system administrator.

Fingerprint Performance Requirements
While the EES Central Systems provide the biometric operations necessary for all procedures during border control, Member States MAY choose to use additional biometric matching algorithms to pre-check the biometric images taken. If Member States decide to do so, the corresponding error rates SHALL be monitored closely.

Please see EU 2019/329 A, Paragraph 1.2.2, Accuracy of Biometric verification, and Paragraph 1.2.3 Accuracy of biometric identification, for:

- The maximum values of FNMR and FMR;
- The false negative identification rate (FNIR) and the false positive identification rate (FPIR).

These thresholds SHALL be configurable at national level to allow for stricter settings when necessary. Please refer to ISO 19795-4 for all the necessary steps to plan, exe-cute and report on biometric testing to check the validity of claims:

- The threshold SHALL be configurable, in accordance with quality requirements, to allow for stricter settings when necessary;
- The fingerprint system has to be calibrated for the security level (FNMR) set within the specific scenario of verification or identification. For this, the provider of the verification algorithm has to provide calibration data (thresholds) based on actual verification or identification performance;
- To ensure the validity of declared values, a provider SHALL provide test results that support each claim. The following requirements apply to those test results:
  - The output of the algorithm SHALL be a comparison score and the result of the verification (the achieved FMR and an indication whether the threshold has been reached) depending on the chosen security level (threshold) of the algorithm;
  - Such performance SHALL be on the basis of images of comparable characteristics (e.g. images with the size and resolution of a typical fingerprint capture deployment for an identity document enrolment);
  - The provider SHALL provide a DET curve and a graph showing the performance of a classification model at all classification thresholds. These claims of the provider MAY verified by an independent test organisation or with an open data set to make the results independent and comparable.

Testing and Evaluation of Fingerprint Capture Systems
Test cases to assess fingerprint sensors in general:

- Performance (speed):
  Assess duration of image capturing on basis of log files (see dedicated section on Logging in Section 2.8.3), ensure that scanner captures images within the specified time limit
- Image quality:
  Assess fingerprints taken by the scanner according to "4C" measurement:
  - Complete (fingerprints are taken completely, no missing parts);
  - Clear (fingerprints are clearly visible);
  - Contrast (fingerprints are high in contrast);
  - Correct (fingerprints correspond to real fingerprints of individual);
- Slap classifier:
  Assess "Ground truth" correctness of slap identification (right/left slap) on basis of log files and expert opinion. Capture right and left hands following or ignoring the scanners' hint of which hand is to be captured. Analyse percentage of cases where the scanner did not notice the wrong hand was presented.
- Test cases to assess PAD of fingerprint sensors:
  - Artefacts
    - Fingertip artefacts:
      paper, foil, silicone, latex, gelatine, wood glue, window painting, acrylic glue
    - Single finger artefacts:
      silicone, latex, gelatine
    - Multi-finger artefacts, complete hands:
      silicone, latex, gelatine

Present artefacts to scanner. Analyse percentage of cases (per artefact class) where the scanner did not notice an artefact was presented. If the scanner is not taking any picture at all, the measurement SHOULD be noted as "scanner noticed artefact".

Also, present low risk fingerprints to the scanner to avoid overfitting of scanners to artefacts by providers. Also, please see ISO/IEC 30107-3:2017, which includes approaches for PAD testing.

2.4. Languages

The following section makes recommendations on the use of languages for the user interface at SSS, e-Gates, ABC and Mobile Systems. The user interface for any system presented to a traveller MUST be multilingual. The language selection MAY be made by means of recognising the nationality in the MRTD. If it is a country that uses several languages, a corresponding selection dialog SHOULD be provided for the traveller. Users with other language preferences SHALL have access to a choice of other languages.

The OS used on the equipment MUST be able to map all the different character sets of the provided language list.

It is RECOMMENDED that the following languages be supported:[5]

- German, English, Russian, French, Spanish, Italian, Chinese, Arabic, Japanese, Portuguese, Turkish.
- Availability of other languages SHOULD be based upon statistics for the BCP.

The possibility to display language from right-to-left is MANDATORY (e.g. Arabic).

2.5. Questions to travellers

At each entry, the traveller MUST be able to fill in an entry survey/questionnaire and SHALL be provided with appropriate support for this purpose. The content of the questions SHALL be determined by EU2016/399 Article 8 (a) points IV-V and each individual MS. C 2019 7131 MAY also be consulted. The multilingual user interface needed to support Questions to Travellers MUST be available in all the chosen languages. In some cases, defined by the Member State, the procedure may be carried out through verbal exchanges between the traveller and the BG.

The framework of the centrally configurable questions SHOULD be the same whether asked manually at an MBC or Mobile System, in self-service mode at an SSS, ABC or Mobile System (Digital Mobile Equipment). A touch screen monitor SHOULD be used for this purpose especially for SSS, e-Gates or ABC. It is RECOMMENDED that a touch screen also be considered for MBC deployments to help address language barriers between the Border Guard and the traveller.

5 Note this list was drawn upon practical experiences from different pilots within Europe and therefore might change over time.

The questions MUST be adaptable by the MS at any time to address changing risks and alerts. The formulation of the questions SHOULD be presented in such a way as to gather the responses easily. Questions for which this is not possible SHOULD be simplified for appropriate elements of the user interface (calendar field for dates, input of numbers, etc.) such as:

- Yes/No answers;
- Multiple Choice: Single item selection;
- Multiple Choice: Multiple item selection;
- Input of numbers (i.e. amounts of money);
- Selection of calendar dates;

on the content of questions to be asked to the TCN traveller.

2.6. Management and maintenance

All border control components SHOULD be part of central governance through a server-based system for:

- Changing configurations;
- Updating application software, SDKs, Driver, OS, firmware;
- Applying virus updates;
- Fixes to bugs;
- An automatic distribution of the central configuration to single, all or groups of components;
- Collection of logs and the provision of statistics and evaluations regarding the usage of each component;
- Managing the health of the deployment (system monitoring):
- activate, deactivate, reboot, etc. remotely
- Determining the operational status of each component;
- Failover in case of a breakdown of a server instance.

Each type of component COULD have its own management system or all border control components COULD be managed through a single central point.

2.7. Data Protection

All data at rest and on the move SHALL be protected by proper means (such as encryption), and access to it SHALL be allowed only to authorised MS authorities.

- Chapter 7 of Regulation 2017/2226 concerns rights and supervision on data protection. Whereas Directive 95/46/EC and Regulation (EC) nº 45/2001 fully apply for this Regulation, the provisions of this chapter clarify certain points related to the right of information campaign accompanying the start of operations of the EES; safeguarding data subjects' rights to access, correction and deletion and remedies; the roles of the national supervisory authorities and the European Data Protection Supervisor, including the cooperation between national supervisory authorities and the European Data Protection Supervisor; and the protection of personal data for law enforcement purposes including rules on logging and documentation.
- The General Data Protection Regulation (GDPR) on data security, Article 78 states "Services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders."
- With regard to data storage:
  - the GDPR states in its article 5(e) that "data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')". In Recital 39(10) it also mentions that to ensure personal data are not kept longer than necessary, time limits SHOULD be established by the controller for erasure or for a periodic review.
  - the Entry/Exit System (EES) Regulation (EU) 2017/2226 states in Article 34 that "(1) Each entry/exit record or refusal of entry record linked to an individual file SHALL be stored in the EES Central System for three years following the date of the exit record or of the refusal of entry record, as applicable; (2) Each individual file together with the linked entry/exit record or records or refusal of entry records shall be stored in the EES Central System for three years and one day following the date of the last exit record or of the refusal of entry record if there is no entry record within three years from the date of the last exit record or refusal of entry record; (3) If there is no exit record following the date of expiry of the period of authorised stay, the data shall be stored for a period of five years following the date of expiry of the period of authorised stay. The EES shall automatically inform the Member States three months in advance of the scheduled erasure of data on overstayers in order to enable them to adopt the appropriate measures; (4) By way of derogation from paragraph 1, each entry/exit record registered for third-country nation-

als who have the status referred to in point (b) of Article 2(1) shall be stored in the EES for a maximum of one year after the exit of such third-country nationals. If there is no exit record the data shall be stored for a period of five years from the date of the last entry record; (5) Upon expiry of the retention period referred to in paragraphs 1 to 4, the data in question shall automatically be erased from the EES Central System".

2.8. Logging

All transactions of the various border control systems SHALL be logged. A transaction SHALL cover all information concerning a single subject.

2.8.1. Logging of General Data

The following general data SHALL be logged:

- Type of station (e.g. stationary or mobile reader);
- Location (including unique BCP number);
- Vendor name and version number of hardware and software;
- Error messages.

2.8.2. Logging of Document Authentication Processes

The following elements SHALL be logged in any case (i.e. if they are present after the process has finished):

- Transaction identifiers;
- Component version information;
- Timing information;
- All check results;
- Defects related to certificates;
- Document data that is not related to personal data:
  - Type of document (MRTD, e-MRTD);
  - Age of document;
- Statistical data about travellers that is not related to personal data:
  - Type of Third Country National;
  - Age or age grouping;
  - Group travel;
  - Length of stay.

Logging of additional elements is application specific and needs to be defined by the MS. Specifying the exact requirements SHOULD therefore be conducted together with the responsible Data Protection Officer.

Possible examples for use cases are:

- logging of document information in the case of suspicion of document fraud for deferred analysis, logging of document data forensic application.

2.8.3. Logging of Biometric Processes

During the biometric process the following data SHALL be gathered / created by the application:

- Generic process information
  - Unique transaction ID
  - Fully qualified host name
  - Type of station (e.g. stationary or mobile) and location
    - Each station/border control component MUST have unique ID
    - Each BCP MUST have a unique location identifier
  - Timestamps of start time and end time of transaction
  - Software used (provider name, version numbers, threshold configuration etc.)
  - Error code if process terminated abnormally
  - Transaction references if transaction is related to other previous transactions
  - Information on process nodes within transaction
- Information about biometric processes (identification, verification, enrolment / one node per applied process)
  - Start and end time of process
  - Submit time of backend processes
  - List of modalities used
  - Information about biometric sample (e.g. finger codes etc.)
  - Result of process
  - Quality Score and binary (Y/N)
  - Quality assessment information
  - Number of returned candidates (if applicable); for each candidate include rank, score and threshold information
  - Threshold information regarding biometric operations such as FMR etc.

2.9. Quality control and assurance

Factory testing

It is RECOMMENDED that factory testing be performed on all border control components prior to delivery for acceptance tests by the MS.

Technical acceptance tests SHOULD be carried out in the MS's own environment.

It is RECOMMENDED to perform regression tests after every change on hardware or software of border control systems.

Business testing

End to end testing SHALL be performed (in all Testing, Acceptance and Production environments of Border Control Systems) using the EES playground provided by eu-LISA. Business test scenarios SHALL be established and performed in a dedicated environment before entry into operation. For the new types of component deployments, or BCPs deployed after the EES's entry into operation, regression tests are strongly RECOMMENDED.

If the systems are implemented before the EES entry into operation, formal compliance testing is also MANDATORY.

Security tests
Vulnerability audits and penetration testing are RECOMMENDED. For this purpose, MS will rely on their standard procedures for their sensitive information systems.

Evaluation
For logging requirements, refer to Section 2.8

For testing and evaluation of facial image systems and PAD, refer to Section 2.3.1

For testing and evaluation of fingerprint sensors and PAD, refer to Section 2.3.2

2.10. Health and safety

No equipment SHALL represent any kind of risk for the safety of travellers. A CE certification SHALL be provided for all equipment supplied and deployed at all BCP and for any equipment which has integrated devices such as MBC, SSS, e-Gates, ABC and Mobile Systems.

All equipment SHALL be resistant to fire. All used materials SHALL, wherever possible, comply with applicable fire safety norms and UL 94 V0.

It MUST be impossible for solutions to have a negative electromagnetic influence and the EMC(EU 2014/30) SHOULD be complied with.

Touchscreen displays need to be flush-mounted with the surrounding surface.

Fingerprint scanners SHOULD be easily accessible by BGS or responsible staff to clean and sanitise them between travellers.

Equipment deployed in indoor locations SHOULD operate between 0°C and 40°C (temperature) and 10% - 90% relative air humidity.

Integrated Equipment (such as at MBC, SSS, e-Gates) SHALL NOT have any frontally or laterally protruding modules/parts (i.e. document readers, facial capture systems, fingerprint scanners) that could break off easily.

The Health and Safety of travellers and all personnel SHOULD be considered in the deployed layout of the BCP.

All travellers MUST be properly redirected in case of security incidents. Emergency procedures SHALL be designed to evacuate the traveller in case of material failure (in particular regarding mantrap systems or dedicated corridors in a MBC); doors SHOULD be able to be manually opened by representatives of the border authorities.

2.11. Vulnerability assessment

All security systems, whether electronic or physical, have vulnerabilities. These vulnerabilities may be simple or complex, and require different levels of expertise and resources to exploit. For an attacker with unrestricted time, resources and system access, effectively any security measure can be circumvented. It is thus important to consider vulnerabilities in the context of the risk that a particular threat will be exploited and the likelihood of other, simpler vulnerabilities in other (non-biometric) parts of the system may be exploited instead. No security technique on its own will completely remove all vulnerabilities. Hence, the incorporation of complementary multiple factors and appropriate governance is RECOMMENDED to reduce overall risk. In security terminology, this is referred to as "defence in depth".

It is inevitable that new attack methods will be discovered, and the risk of the exploitation of known vulnerabilities may also quickly increase where new instructions or materials become readily available. For example, the creation of full latex masks, largely indistinguishable as fakes even by human visual inspection, was previously considered science fiction. They can now be ordered over the Internet. This trend will develop in the future, so attackers may not even require any significant expertise in order to undertake quite sophisticated attacks.

A biometric vulnerability to a threat is indicated when both the liveness detection is defeated (where it is available) and when high match scores are observed during an attack. A score above the minimum threshold that could be practically set represents a potentially successful attack.

The following are some core guidelines for any deployment:

- Personal data MUST be deleted from any station (MBC, SSS, e-Gates, ABC, Mobile Systems) immediately after a successful transaction with the national and EU Central Systems.
- Each element of a system (capture, transfer, matching storage etc.) MUST be examined to unearth vulnerabilities. Figure 4 below breaks down a general system that includes the use of biometrics ISO/IEC 30107-1.
- Fraud detection SHOULD look for artefacts that can defeat the liveness tests and obtain the highest similarity scores. The components of a vulnerability assessment process are to select threats and then apply an assessment methodology. This methodology will undertake a testing process for each threat and provide standardised reporting.
- A PAD for fingerprints and face SHOULD be integrated into the deployed pre-enrolment solutions as a minimum.
- No deployed component SHOULD provide any external data interface which might be used by unauthorized persons.
- The location of a deployment SHOULD be equipped with surveillance cameras which MUST provide a general overview as well as the area around the pre-enrolment devices so that abusive uses can be detected (e.g. use by more than one person):
    - A separate surveillance camera MAY be provided for the fingerprint scanner integrated into the SSS;

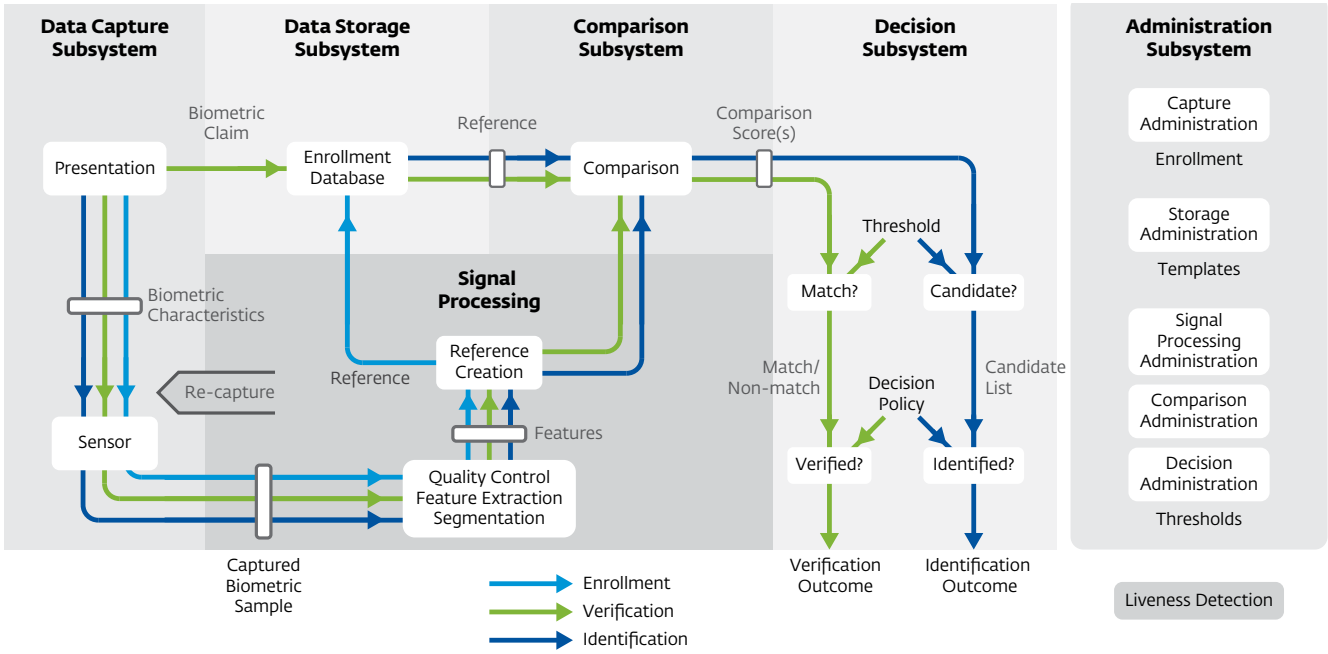

Figure 4: Vulnerability points in a biometric system

- An image (photo) MAY be taken during the taking of the fingerprints, so that the control officers are able to assess whether the fingerprints were taken by the person at the SSS or by another person;
- The SSS MAY be able to detect whether multiple persons were present at the SSS during a single SSS pre-enrolment process;

The live CCTV image data SHOULD be integrated into the border control monitoring process, and stored for potential re-examination/replay, in case of spoofing attempts. It is RECOMMENDED that the CCTV data is footage be stored according to national and EU regulation on privacy issues and personal data storage, please refer to Section 2.7.

PAD tests for the deployed system SHOULD be integrated into the acceptance process for any border control component. If weak points come to light, they SHALL be remedied.

- It is RECOMMENDED that PAD tests be undertaken on a regular basis throughout the duration of the deployment.

2.12. Training

The BG SHALL undergo training courses (online or face-to-face, organised at national and European level) to have deep knowledge of the EES Regulation and EES technology, at least the part of interest. This will allow them to perform tasks and also to provide correct information to users (regulation, number of entries allowed, number of days remaining or allowed).

3. Specific requirements for border control scenarios

3.1. Manual Border Control (MBC)

According to EU 2017 2225 Article 8b par. 4 and 5, a TCN MUST be referred to an MBC:

- If their MRTD contains no chip, the authenticity and integrity of the chip cannot be confirmed or the travel document contains no facial image recorded on the chip;
- If the checks on entry or exit reveal that one or more of the entry or exit conditions have not been met;
- If the results of the checks on entry or exit call into question the identity of the person or if they reveal that the person is considered to be a threat to the internal security, public policy or international relations of any Member State or to public health, or;
- In case of doubts.

In addition:

- Where only parts of the border checks are carried out through an SSS and the traveller is directed to an MBC, the border guard has to verify whether the travel document used at the SSS corresponds to the one held by the person standing before that border guard (EU 2017 2225 Article 8b par. 7).

3.1.1 Technical and performance requirements for border control equipment

Architecture and infrastructure

- Local installed workstations MUST have enough processing capacity and physical data interfaces to connect all peripheral equipment, as a minimum:
  - Full page document reader, please see Section 2.2.2 for requirements;
    - Document readers MAY read boarding cards to process Departing Travellers
    - Document reader hardware module MUST be installed inside of the booth, MUST be controlled and operated by the workstation/border guard officer within the border control booth and MUST not be reachable by the traveller
    - Document readers MUST be installed in such a way that their functionality cannot be disturbed by extraneous light;
  - Facial Capture system, please see Section 2.3.1 for requirements;
  - 4 fingerprint (slap) reader, please see Section 2.3.2 for requirements;
- The workstation MUST be managed and technically supervised by border control authority:
  - Most workstations will be dedicated to First Line traveller processing;
  - Some workstations will be dedicated to Second Line traveller processing;
    - These workstations MAY have additional peripherals to support their investigative work;

- All data exchanges MUST be through a secure network linking the Manual Border Control (MBC) to national Central Systems under governmental control;
- Log data MUST be generated, please see Section 2.8.1;
- The chosen operating system (OS) MUST have a maintenance contract and be regularly delivered with all relevant security services and update packages;
- Access to the Workstation MUST be impossible for non-authorised persons.

The following is RECOMMENDED:

- Dedicated workstations are made available to follow the ongoing technical and business processes. These MAY be located locally at the BCP or centrally;
- A general monitoring system for all deployed MBC. The monitoring MAY be locally at the MBC or centralised at a separate location.

Document authentication
For requirements on MRTD authentication, please refer to Section 2.2

Biometric capture and verification
For general requirements on biometric capture and verification, please refer to Section 2.3.

- The deployment of biometric capture devices SHOULD NOT interfere with the traveller flow and interaction with the Border Guard.
- Normal activities at the border control booth (e.g. handing out travel documents, capturing facial images and fingerprints) SHOULD NOT be affected by the presence of biometric capture systems which face the traveller.
- The booth MAY have voice messaging capabilities to support verbal communication between traveller and the Border Guard.
- The biometric capturing systems MUST be controlled by the workstation within the border control booth.
- Log data MUST be generated, please see Section 2.7.

Facial Capture at the MBC
- It is RECOMMENDED that the facial capture system be mounted outside of the booth in such a way that (glass) reflections are avoided.
- Moving parts MUST NOT be reachable by the traveller.
- The camera SHOULD face the traveller, who SHOULD NOT need to change her/his essential orientation/position.
- While being used, the facial capture system MUST be visible by the operating border guard.
- The system SHOULD support both an automatic capturing process and a manually controlled capturing process.
- A screen dedicated for the traveller (digital mirror) MAY help with the placement of the traveller into the correct position.
- The camera MUST detect if more than one person is being captured.
- A lighting survey for the traveller's location at the booth MUST be undertaken to ensure that there is sufficient lighting available to meet the requirements stated in Section 2.3.1.

- The facial capture system MUST be able to capture travellers from 120 cm to 200 cm height without any manual adjustment.
- In average, a facial capturing process (good light conditions, trained traveller), SHOULD NOT take longer than seven seconds.

Fingerprint Capture at the MBC

- The fingerprint capture system MUST be mounted outside of the booth.
- The system SHOULD face the traveller, who SHOULD NOT need to change his/her essential orientation/position.
- While being used, the fingerprint capture system MUST be visible to the operating border guard.
- The system SHOULD support both an automatic capturing process and a manually controlled capturing process.
- On average, a fingerprint capturing process SHOULD NOT take longer than 10 seconds. The time needed for response from (biometric) backend-systems is NOT included in this range.

3.1.2. User interfaces

The interface provided to the Border guard SHOULD support:

- Traveller data enrolment, automatic launch of searches and display of results for the appropriate workflow;
  - The workflow SHOULD start from MRTD authentication;
- Automatic launching of peripherals during the workflow and interaction with the traveller;
- Additional tools/workflows to address issues occurring in the business process;
- Communication with Second Line officers and monitoring services when help is required.

3.1.3. Operational and process requirements

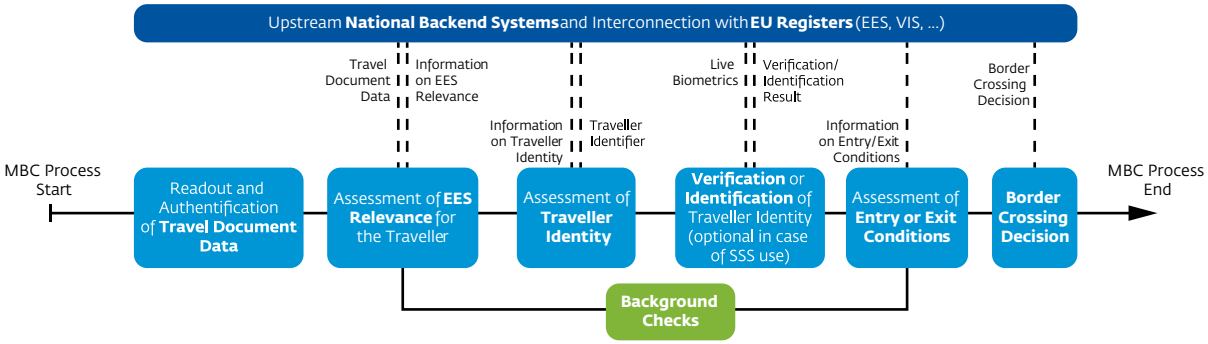

Figure 5: Generic EES Operational Process

The border control process at an MBC starts when the officer places the traveller's travel document on the document reader. If no travel document is present, the traveller is immediately transferred to the Second Line.

Throughout the process, the officer always has the option to transfer the traveller to the Second Line if any problems or inconsistencies preventing the traveller from crossing the border are encountered.

The authentication of the travel document starts with optical document checks, followed by the remaining document checks according to Article 8c of the SBC Amendment and additional national criteria.

In contrast to SSS and ABC, if the MRZ digit check fails the officer can correct wrong characters in the MRZ before sending a request to start the border control to the national Central System (CS). In response to the first request, the national CS determines the traveller type and sends information about the EES relevance and potentially pre-enrolled data for the traveller to the client. If the traveller is EES relevant the national CS automatically starts or continues an EU-WFE transaction. Meanwhile at the MBC, the client starts further background checks and the officer can assess pre-enrolled data, if present, and decide whether to use it as base data for the border control transaction.

The next step is to determine the traveller's identity for EES relevant travellers. For this, an alphanumeric search, based on the MRZ information, is started within both the EES and the VIS. The national CS sends the resulting list, filled in with possibly matching identity entries and requests, to the client.

If one or more identities are found the officer has to assess them and select the one which corresponds to the traveller. If no entry fits or no candidate entries are found, a biometric identification is started and the officer needs to acquire both the facial image as well as the fingerprints of the traveller. If a corresponding identity is selected the officer only needs to capture one biometric characteristic of his/her choice to start the biometric verification of the selected identity.

After the traveller's identity is clarified the officer can assess the information about entry/exit conditions. This can include visa applications for visa holders as well as visa exempts, and the EES calculator results, which also takes into account all stamps for previous border crossings. The officer needs to check whether the traveller is allowed to cross the border or if the TCN currently or previously exceeded the allowed duration of stay.

Additionally, the officer has the option to add the most recent entry stamp during the transition period after the launch of the EES. After all checks have been conducted and the officer has assessed the resulting information and processed each request from the EES, it is possible to make an informed decision about the border crossing and complete the border control. With the decision made, a new border crossing entry with a timestamp, the decision itself, the place of border crossing and in case of Visa Holder (VH) travellers a visa sticker number is added to the traveller's EES file and the EES transaction, together with the border control process itself, is finished.

The assessment of the border crossing decision takes all the information contained in the responses from the national CS (and EES) as well as the locally available information into account. These include but are not limited to:

For TCNs concerned with the EES (TCNS_EES):

- the results from the EES Traveller File verification (including EES facial image verification);
- the need to update the biometrics in the EES Traveller File;
- other calculator results (e.g. overstayer flag).

For all traveller types:

- the border crossing message (in particular its availability);
- national background system check results;
- the availability of messages from the national background system (timeouts);
- the local verification result of live facial image against the electronic chip's DG2 (facial image);
- the facial image verification result between VIZ and e-MRTD;
- the client background checks;
- the document check results;
- a hint in case of a technical error whilst the traveller was in the mantrap area.

3.1.4. Supervision

For MBC, if performed in one step, monitoring is not required as it is performed directly by the Border Guard who will oversee all steps. In case of using a first step for pre-enrolment/pre-control performed through an SSS, monitoring MAY be supported by CCTV surveillance; see Section 3.2.4, SSS Supervision paragraph.

Three levels of monitoring SHALL be implemented:

- Functional: this allows the BG to exchange with the SSS or ABC when the traveller uses those systems; the BG gets useful information (for instance, issues with the traveller) and is allowed to carry out the appropriate actions when necessary (for instance, order the ABC to let the traveller pass through in some cases), or give the traveller certain instructions (through an intercom for example);
- Technical: the BG has to be informed of any incidents;
- Surveillance: the BG SHALL be able to detect any suspicious event.

In some cases the team in charge of equipment maintenance can also implement various tools to check the activity of the systems.

3.1.5. Fall back

The MBC SHOULD be informed about the nature of the incident through a management interface and the MBC SHOULD restart the entire process for the traveller or resume it from the point where the incident occurred.

In case of an incident (unavailability of any software component - EES Central System, NUI or national border control application - network or mere material issue), the system has to be switched to the offline mode.

The BG is informed about the nature of the incident through her/his interface and can restart the entire process or resume it at the point where the incident occurred.

3.1.6. Enrolment

All transactions at an MBC SHOULD meet the data quality requirements and processes of an enrolment process:

- MRTD and document authentication, refer to BSI-TR03135 and ICAO 9303;
- Facial image capture and process of verification between the traveller and the e-MRTD;
- Fingerprint capture;
- Questions and other information supporting the workflow for their individual status.

3.1.7. Verification

Biometric verifications (comparisons with the information stored on the chip and in the Central System) are performed through the technology available (camera or fingerprint scanner). If verification by the leading biometric fails and a second technology is available, a second verification can be performed through this technology.

3.1.8. Handling exceptions

The management of exceptions is strictly connected to the training of the local staff (BG or facilitators) assigned to work at the EES (SSS, e-Gates, SBC, MBC). Every MS SHOULD plan training sessions to help front-office staff handle exceptions such as families with minors under 12, EU nationals, travellers holding RP, travellers not eligible for the SSS because not in possession of an e-MRTD, disabled travellers or any other element that deviates from the ideal process. Single parts of the great body involved in the management of the EES SHOULD act in autonomy but also in synergy to maintain information flow. See also "Fall back" procedures in all BCP solutions (MBC, SSS, Mobile System, ABC and e-Gates).

3.2. Self Service Systems (SSS)

According to EU 2017 2225 Article 8b, and EU 2016 399 Article 8a(1), as of the date of the EES coming into operation, TCNs will be able to use an SSS (e.g. a kiosk, see Section 1.5.2 for definition) to pre-enrol data to carry out such border checks when all of the following conditions are met:

- The travel document contains an electronic storage medium (chip) and the authenticity and integrity of the data on the chip have been confirmed using the complete valid certificate chain. Please see Section 2.2.3.
- The travel document contains a facial image recorded on the electronic storage medium (chip) which can be technically accessed by the Self-Service System (SSS) so as to verify the identity of the holder of the travel document, by comparing that facial image with her/his live facial image.

The results of the border checks carried out through an SSS always need to be made available to a border guard. The border guard who has to monitor the results of border checks SHALL be in charge of detecting any inappropriate, fraudulent or abnormal use of the SSS and, if necessary, directly refer the person to the MBC, where a BG SHALL proceed with further checks. EU 2017 2225 Article 8b par 8.

Surveillance SHALL be implemented where the SSS are deployed to allow overhead surveillance and/or close surveillance of the use of the SSS, especially during the fingerprint capture process, by CCTV and the BG.

3.2.1. Required Information for a successful transaction

A travel document containing an operational electronic chip with data confirmed using the complete valid certificate chain.

Biometric TCN data recorded on the chip of the travel document;

TCN biometric data captured from the SSS;

Additional information about the TCN:

- VISA related data;
- FTD related data (Facilitated Transit Document)

Responses to questions;

Entry or exit flag.

3.2.2. Results

A TCN who used an SSS for carrying out their border checks MAY also be authorised to use an e-Gate (EU 2017 2225 Article 8b par. 6). In such a case, a corresponding enrolment of the entry/exit record and the linking of that record to the corresponding individual file pursuant to EU 2017 2226 Article 14 SHALL be carried out when crossing the border through the e-Gate (in relation to persons whose border crossing is subject to enrolment in the EES). Where the e-Gate and the Self-Service System (SSS) are physically separated, a verification of the TCN SHALL take place at the e-Gate in order to verify that the person using the e-Gate corresponds to the person who used the SSS. Verification SHALL be carried out by using at least one biometric identifier.

3.2.3. Technical and performance requirements for border control equipment

Architecture and infrastructure

An SSS system consists of several components. The SSS MUST have:

- Biometric capture devices: facial capture system and fingerprint scanner. Please see Section 2.3:
  fingerprint scanners MUST be installed in such a way that their functionality cannot be disturbed by extraneous light, and MUST work under optimal temperature conditions;
- Full page document reader (Please see Section 2.2.2):
  Document readers MUST be installed in such a way that their functionality cannot be disturbed by extraneous light;
  For ergonomic reasons, the support surface of the document reader MUST be approximately 85-100 cm above the floor. It is RECOMMENDED that the height of the capture surface of the document reader SHOULD be 90 cm (+/- 10%);
  It is RECOMMENDED that the SSS also be able to read visa stickers and 2D barcodes from paper or a smartphone/tablet. MS MUST evaluate whether the doc-

ument reader is also used for these or if another reader is integrated into the SSS to support the reading requirements.

- Touchscreen user interface:
  The touchscreen display SHOULD be positioned in such a way that the next traveller in the queue in front of the SSS cannot look directly at the display. A vertical or almost vertical installation of the operating display is NOT permitted;
  - It is RECOMMENDED that the screen be at least 15 inches, PREFERABLY 19 inches landscape, to ease the data entry process
- Solution for monitoring biometric accuracy performance (EU 2019/329);
- All data exchanges MUST be through a secure network linking the Self Service System (SSS) to national Central Systems under governmental control;
- SHALL NOT require on-site assembly of parts.

and MAY have components including but not limited to:

- User interfaces (monitors, LED signals, audio devices);
  - It is RECOMMENDED that active signals be given to the traveller as to which component for data capture (fingerprint scanner, e-MRTD reader) has to be used in the workflow process: this MAY be a combination of visual aids on the user interface and the use of flashing LEDs integrated around the appropriate component to indicate that it is ready for use;
  - It MAY have a light, which would indicate that the person using the SSS needs assistance when pressing an assistance button.
- Processing units and network devices (PC, controller, hubs);
  The installed hardware (e.g. PC) for process control and communication with the hardware modules MUST be as maintenance-free as possible (e.g. fanless) for use in a warm and enclosed kiosk which needs external ventilation;
- Integrated cameras/sensors for local surveillance (CCTV) of traveller data capture;
  - The captured images are intended to identify whether presentation attacks are applied, in particular to the fingerprint capture system;
  - The camera system MAY capture an image of the fingerprint capture area at the moment of each finger capture attempt;
  - The images MAY be cached locally on the Self-Service System (SSS);
    - A maximum of 100 ms SHALL be allowed to elapse between the fingerprint capture attempt image and the capture of the surveillance camera system;
  - A colour camera SHALL be used for the fingerprint capture surveillance;
  - The camera SHALL be capable to capture images with a resolution of at least 1280 x 720 pixels;
- Indicator lights and an instructional user display;
- Integrated PAD and Liveness detection solutions.
- A monitoring and control solution.

It is RECOMMENDED that an SSS does not exceed the following dimensions:

- Maximum width W= 65 cm (outside)
- Maximum depth T= 70 cm (including all components)
- Maximum height H= 200 cm

    - Note that if a floor slab is installed, it can increase the height 10 cm beyond the above values in depth and width.
    - Note that some public areas such as airports have height restrictions for individually deployed equipment for health and safety reasons, e.g. 1.5 metres, to ensure all-round visibility.
- The area load SHOULD NOT exceed 200 kg/m²

It is RECOMMENDED that:

- A general monitoring system be deployed at all SSS. The monitoring MAY be locally at the SSS or centralised at a separate location.

Design Considerations

An indicator light MUST be installed in the SSS to show the traveller whether the SSS is in operation (e.g. green indicator light) or not (e.g. red X).

To prevent travellers from briefly depositing and possibly forgetting objects during usage of the SSS (e.g. handbags, document folders, etc.), potential storage areas on the SSS MUST be excluded or appropriately slanted.

The kiosk SHALL be designed in a way that it can be easily serviced and that no moving parts are accessible to the traveller using the kiosk.

It is RECOMMENDED that the fingerprint scanner and MRTD reader not be arranged/installed one behind each other.

- The spatial configuration of the fingerprint capture system SHALL be optimal for primary right hand acquisition.
- The spatial configuration of the fingerprint capture system SHALL allow the capture of left hands.

The document reader SHOULD have an entry guide to make the kiosk easy and intuitive to use for non-trained travellers. The guide MUST ensure that a protective cover on an MRTD MUST NOT be used.

The design SHOULD be modular and all mechanical and hardware components MUST be reliable, robust and designed to meet anticipated load and throughput for the lifetime of the hardware (RECOMMENDED minimum of 5 years, planned project lifecycle of 5-10 years is normal). Modularity helps to guarantee flexibility in updating and replacement of components (either to update the SSS or to replace components).

SSS systems are installed in public areas, so appropriate mechanisms against tampering and vandalism SHOULD be implemented. This includes:

- The use of secure locked panels for accessing the interior of the system:
    - Maintenance access MUST be designed in such a way that access MAY be guaranteed at every installation option (line, back to back, in a circle);
    - Opening a maintenance door MAY trigger a warning signal to the monitoring system, to avoid unauthorised access;

    - On opening a maintenance door, the kiosk MAY be automatically blocked and not be usable by travellers and only accessible by an administrator. Once the door is closed, the kiosk MUST return into operation mode only after activation performed by an authorised user.
- Materials and parts SHOULD be scratchproof and impact- and water-resistant to a reasonable extent. The user guidance display SHOULD be usable over the entire life cycle of the SSS without any impairment during use due to scratches. This MAY be achieved by using display protection foils that can be easily replaced during maintenance.
- The material and surfaces of the system SHALL be selected in such a way that cleaning of the system (by cleaning staff of an external service provider/airport operator) can be easily carried out. If there are special cleaning requirements, these MUST be specified.

The physical parts of the SSS system MUST comply with the applicable health and safety requirements. Please also refer to Section 2.10.

- SSS systems SHOULD make the best use of available space in a way that caters to all users.
- The installation SHOULD be as non-invasive as possible for the existing infrastructure. This covers needs including drilling, mounting of additional barriers and wiring requirements (power and data).
    - Supply lines (electricity, network) MUST be able to be laid according to the local infrastructure (port) specifications, either via the ceiling (e.g. by enclosing them in a stainless steel pipe), via connections in the floor or at the rear of the SSS.
- The SSS equipment location SHOULD be appropriate to avoid process interference such lighting and glare issues.

Document authentication
For MRTD authentication requirements, please refer to Section 2.2

Biometric capture and verification
For general requirements for biometric capture and verification, please refer to Section 2.3.

Facial Images
For requirements for facial capture systems and facial images, please refer to Section 2.3.1

The SSS MUST ensure a full frontal face capture (ISO/IEC 19794-5:2011) and capture facial images from travellers ranging from 120 – 200 cm in height, so the SSS MUST incorporate a solution which captures facial images within this height range from a distance of 40cm–80cm (the capture distance for an SSS).

Fingerprint Images
For requirements for fingerprint capture and fingerprint images, please refer to Section 2.3.2

For the usage in the SSS the following additional requirements MAY be considered:

- During the fingerprint capture process, multiple persons within the reach of the fingerprint capture system of the SSS MAY be detected;
- The multiple person detection result MAY be cached locally on the SSS;
- A maximum of 100 ms SHALL be allowed to elapse between the fingerprint capture attempt image and the capture by the surveillance camera system.

Integration

Software
It is RECOMMENDED to target 35 complete SSS transactions per hour. Thus, the user interface and data capture processes MUST be efficient and MUST run in parallel if at all possible.

It is RECOMMENDED that animations of how to present the MRTD for reading be the starting point, before language selection.

- This will support a fast redirection of a traveller who may not be allowed to use the SSS (EU-Citizen, non e-MRTD, under the age of 12).

When a transaction is abandoned (no usage for 30 seconds), it is RECOMMENDED that the failed transaction be logged and the SSS reset for the next traveller, with an override to allow the next transaction to start. In this case, this information (failed transaction) has to be shown on the display to inform the traveller.

The design of the user interface SHALL support the capturing process in the best possible way, and the way the following devices work:

- document readers;
- facial capture system;
- fingerprint scanner

SHALL be represented by appropriate animations and continuous feedback on the screen of the SSS. The software SHOULD control LED lights to help guide the traveller as to which device is being used.

In addition, the screen MUST also ensure that the following statuses are indicated in the form of meaningful pictograms and symbols:

- Continuous image recording;
- Successful image capture;
- User instructions for correct positioning.

The information displayed on the monitor MUST be directly and immediately related to the traveller's actions (no continuous slide show).

Quality control and assurance
Please refer to Section 2.9

3.2.4. Operational and process requirements

Process Flow

At any time in the process the traveller can be redirected to the MBC by the supervising Border Guard.

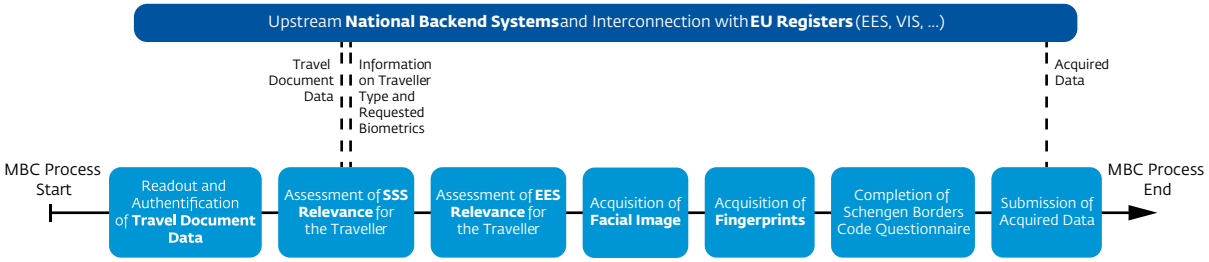

Figure 6: SSS Process Flow

To initiate the border control process at the SSS, the traveller places the passport on the document reader, and the correct language can be determined. In the case of non-translation into the language extrapolated from the nationality of the passport, the traveller SHOULD choose the language from a list of those available.

The readout and authentication of the travel document data begins with the optical document check (please see Section 2.2). If the Machine Readable Zone (MRZ) digit check fails in the first attempt, a second attempt is made in order to eliminate potential optical reading errors due to poor presentation of the travel document. This is followed by reading the MRZ data from the chip and performing the remaining document checks, provided the travel document is an e-MRTD and the MRZ digit check succeeded.

At the same time, the traveller's SSS eligibility is checked (please see Section 2.1 for eligibility guidelines). If the MRZ indicates, for example, that the traveller belongs to the group of FOM travellers or is not old enough to use the SSS (the current lower bound for the age is 12 years according to Article 8c of the SBC Amendment), the traveller is redirected to ABC and MBC, respectively, in order to proceed with the border control process. The process also specifies the optional definition and evaluation of national criteria leading to an exclusion of the SSS usage in case of non-compliance with the configured rule set.

Furthermore, traveller type is determined in a national central level as far as possible through a backend system, to be completed if necessary by questions to the traveller (through the questionnaire or by proper assistance). This is used to determine whether the traveller is registered in an NFP or holds a Residence Permit (RP). In these cases, the traveller is redirected to an ABC or an MBC, respectively. Depending on the document check results and the traveller type, the EES relevance is assessed for deciding on the initiation of EES communication in parallel to the SSS process. This is the case for all travellers who have not already been redirected to ABC or MBC (e.g. NFP/FOM travellers, Residence Permit Holders (RPHs)) and who use an e-MRTD for which a positive complete certificate chain validation has been completed and which

also contain a readable facial image. For all others, the SBC Amendment does not allow a query to the EES CS.

As an example of a possible technical solution, the data will be pre-enrolled in the national Central System and only be definitively stored in the EES CS upon being verified by a border guard. Therefore it is ensured that the data is handled in accordance with the rules defined by the SBC Amendment, while still allowing the SSS to be used as a means to speed up the process at the MBC.

All information collected so far (e.g. MRZ, facial image data from the travel document, EES relevance) is sent to the national CS and added to the (newly created) cached dataset, which is a representation of all the data about the traveller on that level. From this point on, the SSS MAY send status update messages to the national CS, communicating errors and a premature termination of the border control process when the process is aborted due to technical errors.

While background checks are performed in the national CS and the facial image of the Visual Inspection Zone (VIZ) is verified against the e-MRTD, a new EU-WFE transaction (if relevant) is initiated by querying the EES with alphanumeric data from the SSS process. One of the results which MAY be returned by the EES is the "missing hand" status that is used to create a fingerprint acquisition message defining which hand slap SHALL be acquired by the SSS.

Finally, the national CS process is completed by sending this message and a Dataset Identifier to the SSS. In parallel to the described processes in the BCMW, the SSS acquires a high-quality facial image of the traveller and evaluates the age. Immediately afterward, fingerprints requested within the fingerprint acquisition message are captured, either for enrolment or for verification. All the biometric data is then sent to the national CS.

There, the live facial image is verified against the e-MRTD and sent to the EES, along with the acquired fingerprints. The last step from the traveller's perspective is to answer a questionnaire to check the entry conditions according to article 5 of the SBC (please see Section 2.5). When the traveller is finally redirected to an MBC, the answers are sent to the national CS, from where the dataset with all the collected information can later be retrieved by the officer to be able to conclude the border control process.

Certain special events leading to a premature termination may also occur during the SSS process. If, for example, the officer supervising the SSS detects inappropriate or fraudulent use at the SSS, the traveller is redirected to an MBC. If technical errors occur during the SSS process, e.g. with peripherals such as the document reader, facial camera or fingerprint scanner, or even with the SSS itself, the traveller is redirected to another SSS device. In addition, network errors can occur; in this case, the process continues after a certain period of time and resends the messages containing acquired data as soon as the network connection is re-established (see also Operational Fallback). In the event of receiving a delayed message containing information about SSS eligibility (regarding the traveller type and the presence of a complete cached dataset), an already started process is aborted for travellers who are not allowed to use the SSS.

Pre-Enrolment
All transactions at an SSS SHOULD meet the data quality requirements and processes of an enrolment process:

- MRTD and document authentication;
- Facial image capture and process of verification between the traveller and the e-MRTD;
- Fingerprint capture ;
- Questions and other information supporting the workflow for their individual status.

If the traveller CAN NOT follow or is unable to self-capture the required quality of the facial image or fingerprints, they MUST be directed to MBC.

Verification
Verification of alphanumeric data will take place at the CS-EES.

Verification of the live captured facial image against the facial image of DG2 and bio-data page MAY take place at the MS-CS or locally in the SSS.

Supervision
Access to the SSS SHALL be monitored and supervised by BGs. Physical Monitoring of the SSS deployment MAY be supported by CCTV surveillance. It is RECOMMENDED that this be in place to prevent fraudulent use of the SSS with the following requirements:

- A CCTV colour camera system SHALL supervise the area around the SSS deployment.
- The camera images SHALL support manual monitoring and reviewing of the SSS usage to help determine whether more than one person was in range of an SSS during a data capture process.
- The images SHALL be cached locally on the local monitoring system.
- The use of CCTV will allow a review of any potential fraudulent behaviour (i.e. during the document scan process, facial image capture process and fingerprint capture process).
- It is RECOMMENDED that the CCTV footage be stored according to national and EU regulations on privacy issues and personal data storage; please refer to Section 2.7.
- The ability to capture short footage for longer storage to support an investigation is RECOMMENDED.

User guidance
Traveller Information and Guidance
For the traveller, there are three ways of guidance:

1. The process flow for the SSS actually starts before the traveller uses the SSS. It is RECOMMENDED that steps be performed such as delivering information to travellers provided through their carriers before arriving at the BCP, to help avoid overcrowding of the SSS area. When at the BCP, travellers SHOULD be directed

to the correct lanes (travellers not involved in the EES such as EU citizens, holders of residence cards SHOULD be directly sent to the appropriate border checks). Therefore, direction signs and visualisation aids SHOULD be in place.

2. The use of the following MAY help process travellers faster at the SSS:
    - An facilitator MAY start explaining the use of the SSS, ask travellers to prepare travel documents, to take off sunglasses, hats etc.; he/she could direct special groups to manual border checks or give basic explanations in addition to the written information and user interface ones:
        - Facilitator numbers SHOULD be proportionate to space and to the number of travellers expected to arrive at a given time;
        - The use of Advance Information (e.g. API, PNR) and border crossing statistics data MAY help Border Authorities anticipate the expected number of TCN travellers;
    - Use of Mobile Services (Digital Mobile Equipment and application for Travellers):
        - The development of an APP for travellers to use which MAY tell them where to go (if they are TCNS) at the BCP;
        - Allow TCNs to complete a questionnaire, for submission:
            - at the SSS or MBC through the use of a QR code;
            - to a service for retrieval through a QR code at the SSS;
        - The proper human assistance when using the SSS;
        - The information provided by the system itself (through the screens mentioned above).
3. SSS SHOULD also provide further information for travellers already registered in the system, displayed in the national language of traveller where possible, or in one of the most popular languages, such as:
    - validity of documents and anticipated expiry of document (if appropriate);
    - need to update data related to travel document;
    - number of entries available or number of days still remaining following a previous entry.

Border Guard

For the BG, information SHALL be delivered through her/his user interface. The BG SHALL be trained online or during face to face sessions in how to access and understand the information. (Please see Section 2.12.)

Integration

- Configuration/topology
- Physical infrastructure considerations
- Environmental factors
- Maintenance
- Other

Operational Fallback
If and only if the EES Central System (CS-EES) is not available, the information has to be introduced according to the regulation in offline mode. A complete set of data (alphanumerical, biometric – facial image and fingerprints) is captured. The data MAY be stored at any national level (NUI, National System, local server, workstation), according to the level of the unavailability. Once the issued is fixed, the stored information MUST be processed and transmitted to the CS-EES as information processed in an offline mode. If the NUI is not available, the information has to be registered manually by the BG using a special form and stamp documents.

The Border Authority MUST implement the necessary steps to guarantee the security of the procedures and the protection of data, and prevent unavailability of National Systems.

Quality control and assurance
For logging and statistics:

- Please refer to Section 2.8.

For Data protection:

- Please refer to Section 2.7.

3.3. e-Gates & Automated Border Control (ABC) Systems

3.3.1. Technical and performance requirements for border control equipment

Architecture and infrastructure
The ABC system consists of an SSS and an e-Gate, as defined by Article 1 (1) of the SBC Amendment, implementing the parallel two-step ABC process.

There are 3 types of ABC configuration (refer to Frontex ABC BPTG, par.3):

- One-step ABC system
  - The traveller is able to complete all transactions (i.e. document, biometric verification and border passage) in one single process without moving to another stage.
  - This usually takes the form of a mantrap e-Gate.
- Integrated two-step ABC system
  - The traveller verifies the document at the first stage, and then, if the document verification is successful, moves to a second stage within the same physical structure where the biometric verification is carried out.
  - This is invariably implemented using a mantrap e-Gate.
- Segregated two-step ABC system
  - The processes of document authentication and traveller verification are completely separated from the passage through the border control.
  - This typically takes the form of a kiosk for verification of the document and the holder, while border passage occurs at an e-Gate through the use of a temporary token.

The architecture varies according to the type of ABC, but the e-Gate is always monitored by the central monitoring system. Separated systems are dealt with in the chapters related to the SSS (page 56, section 3.2) and e-Gates (page 67, section 3.3).

Technical components:

- The client systems (ABC or e-Gates) to be used by the traveller;
- The MS-CS acting as an interface between the client systems and the European systems;
- The BG's tool.

All data exchanges MUST be through a secure network linking the e-Gate & Automated Border Control (ABC) System to national Central Systems under governmental control.

It is RECOMMENDED that a general monitoring system be deployed at all e-Gates & Automated Border Control (ABC) Systems. The monitoring MAY be locally at the e-Gate/ABC or centralised at a separate location.

Document authentication process

For requirements for document checks, please refer to Section 2.2.

Document readers MUST be installed a way that their functionality cannot be disturbed by extraneous light; for ergonomic reasons, the support surface of the document reader SHALL be approximately 85-100 cm above the floor. It is RECOMENDED that the height of capture surface of the document reader SHALL be 90 cm (+/- 10%). It is RECOMENDED that ABC MAY also read visa stickers, 2D barcodes from paper or smartphone/tablet. An indicator light MUST be installed in the ABC to show the passenger whether the system is in operation. The document reader SHOULD have an entry guide to make the ABC easy and intuitive to use for non-trained travellers. The guide MUST ensure that a protective cover on an MRTD MUST NOT be used. The design SHOULD be modular and all mechanical and hardware components MUST be reliable and robust. The physical parts of the ABC system MUST comply with the applicable health and safety requirements. Please also refer to Section 2.10

Biometric capture and verification

For requirements for facial images, please refer to Section 2.3.1.

For usage in mantrap scenarios the following additional requirements SHALL be met:

- The facial capture system SHALL cover at least a height range of 120 cm to 200 cm (if standing in front of the camera system) from a distance range of 60cm to 200cm with sufficient sharpness and with minimal distortion of the captured face.
  - Facial capture SHALL be for verification purposes against an existing facial image of the traveller.
  - The necessary rotation of the person required for facial capture MUST be less than 15 degrees

For biometric requirements for fingerprint images, please refer to Section 2.3.2.The fingerprint capture process SHALL be for verification purposes against existing fingerprint images of the traveller.

User interfaces
There are two types of interface:

- For the BG:
  - a single user's interface (screen) enabling him/her to monitor, supervise and communicate with the ABC system in the case of an integrated system (see dedicated sections under the SSS and e-Gates)
- For the traveller
  - several screens (one for the processing of the MRTD and one for the capture of biometry) providing him/her with instructions and information.

Integration
- Technical integration (software and hardware)

Quality control and assurance
- For Data Protection please refer to Section 2.7
- For testing (including Penetration Attack Detection) please refer to Section 2.9
- For logging requirements please refer to Section 2.8

Evaluation
For testing and evaluation of facial capture system cameras, please refer to Section 2.3.1.

For testing and evaluation of fingerprint sensors, please refer to Section 2.3.2.

For Presentation Attack Detection for facial images, please refer to Section 2.3.1.

The assessment of biometric vulnerability is vital for ensuring ABC border security. While there are currently few examples of detected attacks that have tried to circumvent the biometrics in ABC systems, authorities SHOULD be prepared for significantly increased risks from such attacks in the coming years due to the wider use of ABC systems and increased sophistication of attackers. It will be vital for system assessors to understand how such attacks arise and to know some simple ways to test for potential vulnerabilities.

Potential threats to biometric ABC systems range from the presentation of artefacts, such as a simple picture of a face on a T-shirt, to the reconstruction of a biometric from stolen biometric templates. The threat list will expand continuously as new techniques, tools, skills and materials upon which to base attacks become available. The assessment of the likelihood of an attack succeeding in an ABC system is complex because:

- **Biometric matching is a probabilistic process**
  A combination of user behaviour, environmental conditions and physical ageing of the biometric affect the matching outcomes of a biometric system. This means there is never absolute certainty of identity through biometric means alone. The management of the recognition thresholds of the biometric matching algorithm mitigates the influence of external factors and is performed to arrive at an acceptable trade-off between FMR and FAR.

- **Detection failures**
  Any presentation attack detection system is likely to be probabilistic itself, and thus generate false alerts and false non-alerts, which will lead to the system falsely rejecting or accepting a traveller.

- **Repeatability**
  The success of a presentation attack may rely on many factors that are not inherent in the physical artefact itself. These include environmental changes and attacker techniques.

- **Covert capture**:
  Many biometrics share the property that it is easy to covertly obtain a sample. For fingerprints, this may be by simply raising latent fingerprints off touched surfaces. For faces and irises, high-resolution digital photography may be enough to create an artefact; consequently we cannot consider such biometrics to be secret.

- **Look-alike fraud:**
  An MRTD may be targeted for theft because the fraudster looks similar to the genuine passport holder. This is called look-alike fraud. This type of fraud has also been committed by family members, as siblings tend to look similar and can be particularly difficult to detect based on biometrics alone.

3.3.2. Operational and process requirements

e-Gate Process Flow
Travelers can use e-Gates after an SSS.

For exit of the Schengen Area, all TCNs already registered in the EES (VE or VH) can use e-Gate systems.

For entry to the Schengen Area, the use of e-Gates is allowed for TCNs already registered in the EES under the same conditions as the ones applicable to the ABC systems:

- VE TCNs according to the national regulation (generally from countries without migratory risk);
- VE or VH registered in an NFP.

As underlined in Article 8a of the SBC Amendment, as regards the use of the Entry/Exit System (EES), and in accordance with the interpretation note issued by the Commission with regard to the implementation of this article, there are several ways to pre-enrol first time travellers. This document will reflect two processes:

- The first process consists of an SSS followed by an e-Gate, where the verification of the pre-enrolled data of the traveller is performed remotely by the BG.[6]
- The second process consists of an SSS followed by a Manual Border Control (MBC) or booth, where the BG will perform the verification.

6 Until the development of the EES handbook is completed, the use of e-Gates by first-time registered TCNs is not considered in this technical guide.

Nonetheless, neither of these processes is binding, since verification could take place at any time between the enrolment of the data and the border check, and it is at the discretion of MS to design the process, always in accordance with the SBC Amendment and national regulations.

MS can use the workflow engine or atomic operations (the second possibility seems quite unlikely: an automatic combination has to be set up by the NS at the kiosk and the e-Gate).

The ABC system consists of an SSS and an e-Gate, as defined by Article 1 (1) of the SBC Amendment, implementing the parallel two-step ABC process. Therefore, it is equipped with a document reader and a biometric capture unit for facial image and/or fingerprint acquisition. This enables EES registered TCN travellers, NFP travellers, Residence Permit Holders (RPH) as well as FOM travellers to cross the border automatically using an e-MRTD. While within the scope of these descriptions the first mentioned traveller type (EES registered TCNs without RP or active enrolment in an NFP) MAY use the ABC only in exit direction, the other types of travellers MAY use it for both entry and exit.

Although the e-Gate process runs automatically in the ideal case, it MAY be required for the monitoring officer to intervene in certain cases, e.g. if suspicious activity by the traveller is detected. The officer has the option to influence the process without terminating it prematurely.

To initiate the border control process at the e-Gate, the traveller places the electronic passport on the document reader. Similar to the SSS process, the readout and authentication of the travel document data begins with the optical document check. However, in contrast to the SSS only one attempt for the MRZ digit check is allowed here, with the exception of a wrong document positioning on the reader which COULD be solved with the help of assisting personnel with another attempt. If this fails, the traveller is redirected to an MBC. Otherwise, the MRZ data is read and assessed in regard to the configured requirements, for example the age and nationality of the traveller. For travellers old enough to use the e-Gate (the current lower bound for the age is 12 years according to Article 8c of the SBC Amendment) and who fulfil the additional national criteria that may be required, the document check process is continued. Meanwhile, the traveller type is determined in the national CS for all those who are not already identified as FOM travellers.

The next step is to assess the EES relevance. Since all travellers whose passports do not contain an embedded contactless chip will already have been redirected to an MBC as a result of the document checks, the decision is largely taken based on the type of traveller. NFP travellers and TCNs using an e-MRTD with a positive complete certificate chain are relevant for the EES, whereas FOM travellers and RPHs (regardless of the certificate chain validation) are not. TCNs and NFP travellers without a positive complete certificate chain are redirected to MBC.

All information collected so far (e.g. MRZ, facial image data from the travel document, EES relevance) is sent to the national CS and added to the (newly created) cached dataset. If the e-Gate process is aborted, e.g. due to technical errors or factors pro-

hibiting the use of the e-Gate, a status update message communicating errors and a premature termination of the border control process is sent to the national CS from this point on.

While background checks are performed in the national CS and the facial image of the VIZ is verified against the e-MRTD, a new CS-EES transaction (if relevant) is started. For this reason, the EES is queried with alphanumeric data obtained in the e-Gate document check. The response of the EES in turn is used to determine whether the traveller is properly enrolled in the EES, i.e. a biometric verification against the related Traveller File data is possible. The result of this evaluation is sent to the e-Gate, concluding the national CS process.

At this point in the entry process, all travellers who try to use the e-Gate without fulfilling the requirements (e.g. TCNs without an active NFP enrolment, RP or FOM status) are redirected, according to BCP structure and national implementation, directly to an MBC or an SSS, and all TCNs who are not properly enrolled in the EES according to the evaluation results in the response received from the national background system are definitively redirected to an MBC.

Once the eligibility for e-Gate usage and the EES relevance have been assessed, the traveller enters the mantrap area of the e-Gate, according to BCP structure and national implementation, where local background checks are performed simultaneously with the capture of the facial image and its verification against the electronic chip's Data Group 2 (Encoded Face) (DG2) (facial image). Regardless of the verification result, the acquired biometric data is sent to the national CS (and from there to the EES) to create a border crossing message containing all information relevant for the border crossing decision. This includes, for example, whether the EES communication was successful, the results from the EES Traveller File verification, whether the biometrics in the EES Traveller File have to be updated, the results of the national background system checks, the result of the facial image verification between VIZ and the e-MRTD and other calculator results such as overstayer duration. The exact contents of the resulting message depend on the traveller type.

The process at the e-Gate is concluded when the exit door opens and a final message containing the remaining border control data (e.g. the results of the assessment of the border control decision) as well as the remaining time until automatic creation of an entry or exit record, or sending of a warning, is sent to the national CS.

ABC Process Flow
Travelers MAY use e-Gates after an SSS.

For exit of the Schengen Area, all TCNs already registered in the EES (VE or VH) can use ABC systems.

For entry to the Schengen Area, the use of e-Gates is allowed for TCNs already registered in the EES under the same conditions as the ones applicable to the e-Gate systems:

- VE TCNs according to the national regulation (generally from countries without migratory risk);
- VE or VH registered in an NFP.

As underlined in Article 8a of the SBC Amendment, as regards the use of the Entry/Exit System (EES), and in accordance with the interpretation note issued by the Commission with regard to the implementation of this article, there are several ways to pre-enrol first-time travellers. This document will reflect two processes:

- The first process consists of an SSS followed by an e-Gate, where the verification of the pre-enrolled data of the traveller is performed remotely by the BG.[7]
- The second process consists of an SSS followed by a Manual Border Control (MBC) or booth, where the BG will perform the verification.

Nonetheless, neither of these processes is binding, since verification could take place at any time between the enrolment of the data and the border check and it is at the discretion of MS to design the process, always in accordance with the SBC Amendment and national regulations.

MS can use the workflow engine or atomic operations (the second possibility seems quite unlikely: an automatic combination has to be set up by the NS at the kiosk and the e-Gate).

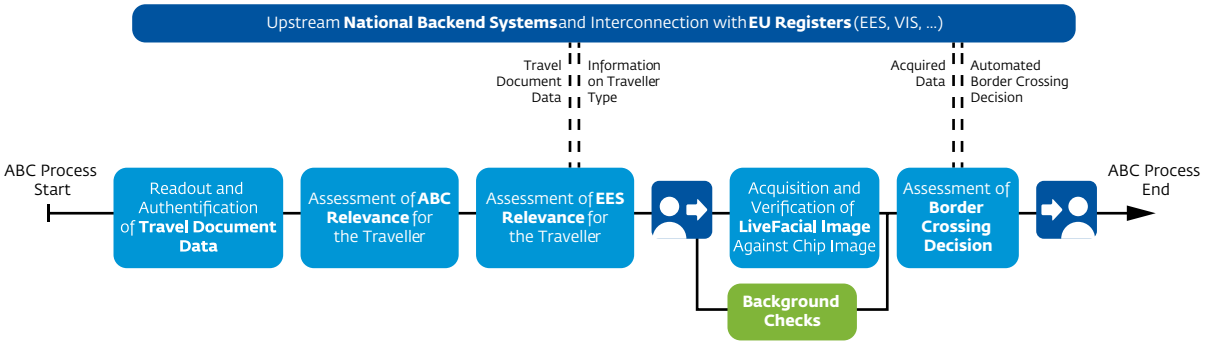

Figure 7: Process Flow

7 Until the development of the EES handbook is completed, the use of e-Gates by first-time registered TCNs is not considered in this technical guide.

The ABC system consists of an SSS and an e-Gate, as defined by Article 1 (1) of the SBC Amendment, implementing the parallel two-step ABC process. Therefore, it is equipped with a document reader and a biometric capture unit for facial image and/or fingerprint acquisition. This enables EES registered TCN travellers, NFP travellers, RPHs as well as FOM travellers to cross the border automatically using an e-MRTD. While in the scope of this description the first mentioned traveller type (EES registered TCNs without RP or active enrolment in an NFP) MAY only use the ABC in exit direction, the other types of travellers MAY use it for both entry and exit.

Although the ABC process runs automatically in the ideal case, it MAY be required for the monitoring officer to intervene in certain cases, e.g. if suspicious activity by the traveller is detected. The officer has the option to influence the process without terminating it prematurely.

To initiate the border control process at the ABC, the traveller places the electronic passport on the document reader. Similar to the SSS process, the readout and authentication of the travel document data begins with an optical document check. However, in contrast to the SSS only one attempt for the MRZ digit check is allowed here. If this fails, the traveller is redirected to an MBC. Otherwise, the MRZ data is read and assessed in regard to the configured requirements, for example in terms of the age and nationality of the traveller. For travellers old enough to use the ABC (the current lower bound for the age is 12 years according to Article 8c of the SBC Amendment) and who fulfil the additional national criteria that may be required, the document check process is continued. Meanwhile, the traveller type is determined in the national CS for all those who are not already identified as FOM travellers.

The next step is to assess the EES relevance. Since all travellers whose passports do not contain a readable facial image recorded on the electronic chip will have already been redirected to an MBC as a result of the document checks, the decision is largely taken based on the type of traveller. NFP travellers and TCNs using an e-MRTD with a positive complete certificate chain are relevant for the EES, whereas FOM travellers and RPHs (regardless of the certificate chain validation) are not. TCNs and NFP travellers without a positive complete certificate chain are redirected to an MBC.

All information collected so far (e.g. MRZ, facial image data from the travel document, EES relevance) is sent to the national CS and added to the (newly created) cached dataset. If the ABC process is aborted, e.g. due to technical errors or factors prohibiting the use of the ABC, a status update message communicating the errors and the premature termination of the border control process is sent to the national CS from this point on.

While background checks are performed in the national CS and the facial image of the VIZ is verified against the e-MRTD, a new CS-EES transaction (if relevant) is started. For this reason, the EES is queried with alphanumeric data obtained in the ABC document check. The response of the EES in turn is used to determine whether the traveller is properly enrolled in the EES, i.e. a biometric verification against the related Traveller File data is possible. The result of this evaluation is sent to the ABC, concluding the national CS process.

At this point in the entry process, all travellers who try to use the ABC without fulfilling the requirements (i.e. TCNs without an active NFP enrolment, RP or FOM status) are redirected to the SSS and all TCNs who are not properly enrolled in the EES according to the evaluation results in the response received from the national background system are redirected to an MBC.

Once the eligibility for ABC usage and the EES relevance have been assessed, the traveller enters the mantrap area of the ABC, where local background checks are performed simultaneously with the capture of the facial image and its verification against the electronic chip's Data Group 2 (facial image). Regardless of the verification result, the acquired biometric data is sent to the national CS (and from there to EES) to create a border crossing message containing all information relevant for the border crossing decision. This includes whether the EES communication was successful, the results from the EES Traveller File verification, whether the biometrics in the EES Traveller File have to be updated, the results of the national background system checks, the result of the facial image verification between VIZ and e-MRTD and other calculator results such as overstayer duration. The exact contents of the resulting message depend on the traveller type.

The assessment of the border crossing decision takes all the information contained in the responses from the national CS (and EES) as well as the locally available information into account. These are, for example:

For TCNs without Residence Permit:

- The results from the EES Traveller File verification (including EES facial image verification);
- The need to update the biometrics in the EES Traveller File;
- Other Calculator results (e.g. overstayer flag).

For all traveller types:

- The border crossing message (in particular its availability);
- National background system check results;
- The availability of messages from the national background system (timeouts);
- The local verification result of live facial image against the electronic chip's DG2 (facial image);
- The facial image verification result between VIZ and e-MRTD;
- The document check results;
- A hit in case of a technical error whilst the traveller was in the mantrap area;
- An intervention hit if the officer decided to intervene.

The assessment begins with the question of whether a biometric update of the Traveller File is requested by the EES. If it is, the officer has to acquire new biometrics at the MBC, preventing the automatic creation of an entry or exit record at the end of the ABC process. In these cases, both the opening of the exit door and adding the border crossing decision to the EES Traveller File have to be performed manually from the monitoring station and from the MBC, respectively.

It is OPTIONAL that the process at the ABC is concluded when the exit door opens and a last message containing the remaining border control data (e.g. the results of the assessment of the border control decision) as well as the remaining time until automatic creation of an entry or exit record or sending of a warning is sent to the national CS. The process MAY vary from MS to MS as it SHALL be based on national decisions.

Verification
The biometric verifications (comparisons with the information stored on the chip and in the Central System) are performed through the technology available (camera or fingerprint capture system). If the verification by the leading biometry fails and a second technology is available, a second verification can be performed using this technology.

If the verification fails, the traveller has to go to the booth. In this case, the BG is informed about this failure (mainly through his/her user interface).

Monitoring
Three levels of monitoring SHALL be implemented:

- Functional: this allows the BG to interact with the ABC when the traveller uses the system. The BG gets useful information (for instance, issues with the traveller) and is allowed to carry out the appropriate actions (for instance, order the ABC to let the traveller pass through in certain cases, or give the traveller certain instructions, e.g. through an intercoms);
- Technical: the BG has to be informed of the incidents;
- Surveillance: the BG SHALL be able to detect any suspicious event.

In some cases the team in charge of the maintenance of the equipment can also implement different tools in order to check the activity of the systems.

It is RECOMMENDED that operational monitoring take place in the following forms:

- Overall passage times (for document reading and validation, and biometric verification);
- Overall performance of the e-Gate;
- Tailgating and presentation attack detection;
- e-MRTD validation (which certificates were able to be processed, cryptographic checks, optical checks, overall schema);
- Downtime of the e-Gate;
- Equipment long-term reliability and its ability to meet anticipated load and throughput for the lifetime of the hardware;
- False Reject Rate (FRR) and False Accept Rate (FAR) analysis;
- Integration testing with the airport and border control backend systems.

Any ABC system SHOULD have the **ability** to generate reports on agreed aspects of system performance including:

- Biometric Events (Score Matching);
- Biometric Quality;

- Volumes (Score Matching);
- Synchronisation (Status);
- Errors and Warnings;
- The reports SHOULD be able to be generated as PDF or HTML;
- Online reports SHOULD be able to be drilled down into to examine the underlying data;
- Report output SHOULD be able to be generated over various date ranges including day, week, month, quarter, financial year, calendar year;
- Reports SHOULD allow user customisation of data columns.

By installing an active monitoring system that looks for deviations in normal operational usage, potential fraud relating to system vulnerabilities can be detected, or attempted attacks can be detected through an analysis of time series data. Furthermore, the examination of audit logs can potentially reveal patterns of internal fraud.

Integration

- Configuration and topologies
- Physical infrastructure considerations
- Environmental factors
- Maintenance
- Other

Fallback

In case of an incident (unavailability of an application - EES or any other, such as SIS – network or mere material issue), the system has to be switched to the offline mode. The traveller is referred to the MBC.

The MBC is informed about the nature of the incident through the interface and can restart the entire process or resume it at the point where the incident occurred.

3.4. Mobile Systems

This section examines how a Mobile approach can be integrated into addressing the need for TCN data capture and verification to meet the requirements of the EES.

Integrating a Mobile approach for border control is now an essential part of the border control infrastructure. It offers an efficient approach at BCPs which are challenging to address such as:

- BCPs which are not used very often;
- BCPs with border checks inside various means of transport such as trains or buses;
- When border authorities need to capture data in difficult situations such as on a boat;
- Establishing a BCP for a short period of time at a location which does not have any infrastructure.

Mobile systems for law enforcement have been deployed for almost 15 years now, and technology has moved on since those early days. Not only is the equipment available

on the market smaller, lighter and more powerful, but data capture processes can be offered to the traveller themselves to help prepare for their arrival at a physical BCP. So a traveller-orientated mobile approach is also touched upon here. However, for this first version of the document, we have prioritised the general and operational requirements of a border guard using mobile devices.

3.4.1. Classification of mobile systems and application scenarios

There are three categories of mobile system:

- Temporarily Stationary Equipment
  These solutions are meant to be comprehensive and easily transported, providing the same functional features as Manual Border Control (MBC) equipment with higher requirements for usage. Besides addressing a TCN identity verification use case, they SHALL provide all enrolment features taking into account all specific environmental conditions at the BCP location(s). It is assumed that this location will be under cover.
- Portable Mobile Equipment
  This type of equipment provides full verification features but the ability to use such devices in the EES enrolment scenario is limited. Usage of Portable Mobile Equipment for the EES enrolment scenario SHOULD be performed when there is no other possibility to perform such tasks with other devices. Usage of Portable Mobile Equipment for pre-enrolment when only biometrics (face and image) with document details are collected SHOULD be also possible with this kind of device.
- Digital Mobile equipment and application for travellers
  This is an application on a standard mobile/tablet where the traveller can pre-enrol their data (or elements of their pre-enrolment data). Once entered into the Application on the traveller's own device, a 2D code can be created which can then be used with a software application operated by the eligible authority as part of the border control process.

Each category is involved in different use cases and with different users, as presented below in Table 1.

Table 1: Mobile System Category Matrix

Scenarios	Mobile System Categories		
	Temporarily Stationary Equipment	**Portable Mobile Equipment**	**Digital Mobile equipment and application for travellers**
Self-service pre-enrolment (by the traveller)	Yes	No	Yes
Supervised pre-processing (by the traveller, with assisting personnel)	Yes	Yes	No
Border control, including EES enrolment (by the BG)	Yes	Yes – mainly used as a workaround if necessary	No
Border control, without EES enrolment (only verification)	Yes	Yes	No
Identity checks	Yes	Yes	No
User Groups			
Travellers (using their own personal device)	No	No	Yes
Assisting personnel (crew, airport personnel using dedicated/certified devices)	No	Yes	No
Official/border guard using official devices (e.g. by border police)	Yes	Yes	No

A more detailed overview of the scenarios is as follows:

- Self-service pre-enrolment (by the traveller)
  - Traveller prepares/provides pre-enrolment data up front:
    - not all pre-enrolment data needs to be captured, the concept is to pre-capture data to help speed the process. For example: responses to questions
    - any biometric capture which might be undertaken in the process (e.g. to tie the data captured on the phone to the physical person using the mobile device) SHALL NOT be submitted to EES. However it could be used in a local biometric matching workflow at the point of data submission;
    - the traveller's personal device SHALL be deemed untrustworthy. This implies that any captured data MUST be verified when submitted and processed accordingly.
  - An SSS which is more portable could be used, i.e. kiosks on wheels or the top half of a kiosk, which could be placed on a table, or a solution which is stored in a suitcase and which could have the same software used in an SSS deployed in a fixed BCP.
- Supervised pre-processing (by the traveller, with assisting personnel):
  - assisting personnel (non-official) MAY support TCN travellers in the use of systems, to introduce their alphanumeric and biometrics data;
  - personnel are trained and authorized by an MS border authority for data acquisition.

- Border control, including EES enrolment (by the BG):
  - enrolment and verification of travellers' identities;
  - e. g. for travellers upon crossing of external borders (e.g. airports, seaports);
  - capture and processing of a traveller's document, alphanumeric and biometric data;
  - enrolment of data in Central Systems (national and EU) and verification against stored data;
  - addresses the need for quality data capture:
    - requires proper equipment delivering high quality document and biometric data;
    - addresses the issue of fraudulent identities in the workflow of the deployed solution.
- Border control, without EES enrolment (verification only):
  - fast processing of travellers, which only have to be verified (TCNs are already pre-enrolled within the EES);
  - addresses the need to handle peaks at BCPs or temporary locations.
- Identity checks:
  - mostly verification of identities using available databases;
  - e.g. ad hoc identity checks and search in Central Systems (national and/or EU);
  - focus on flexibility and mobility of equipment.

3.4.2. Equipment variants for Portable Mobile Equipment

As the category ***Portable Mobile Equipment*** provides several setup options depending on the equipment size, Table 2 presents a more detailed definition.

Table 2: Portable Mobile Equipment Specification Overview

Equipment Size	General specification of the hardware configuration
Small	Standard smartphone on the market (iOS or Android OS COTS product) with integrated camera and LED lighting, NFC/RFID module and optionally connected to external devices using USB and/or Bluetooth
Medium	Standard Smartphone on the market (iOS or Android OS COTS product) in a physical sleeve: • The smartphone is slid into a physical sleeve which integrates peripherals, e.g. FP scanner, document reader, better camera, etc. Handheld, rugged mobile COTS device with integrated peripherals e.g. FP scanner, document reader, camera, NFC/RFID module, document reading capability, smartcard reader, 1D/2D barcode reading etc.
Large	Tablet (mobile ARM platform or x86 architecture) with integrated devices for better data capture quality (e.g. NFC/RFID scanner, document reader, ID/2D barcode reading, contact smartcard reader, camera, LED lighting, single or 2-finger or slap FP scanner)

3.4.3. Technical, Configuration and performance requirements for Mobile Systems

Mobile systems SHALL meet the following general requirements:

- The solution SHALL support at least UMTS (3G, CDMA) as a mobile communication standard. It is RECOMMENDED that a mobile system support 4G/LTE or higher standard. It is REQUIRED for a mobile system to be able to connect with Wi-Fi.
- Transaction Response times SHALL normally be synchronous. Total response time for all operations sent in one step from a mobile system SHALL aim to respond synchronously to queries within less than 10 seconds (measured end-to-end), SHOULD be less than 30 seconds and SHALL NOT exceed 60 seconds. Total response time MAY vary depending on the communication mode used to connect to the MS national Central System.
- Mobile connections tend to be volatile and depend on location. Security of the captured/stored data (even if temporarily) MUST be risk assessed.
- A risk assessment on the security of the Mobile Equipment is MANDATORY.

Specific Technical Requirements for Temporarily Stationary Equipment

- It is RECOMMENDED that Temporarily Stationary Equipment be able to operate for at least 6 hours without any connection to an external power source if its proposed use does not guarantee such an external power source. The mobile system SHALL continue to be usable during the charging of any battery. It is RECOMMENDED that the equipment can be charged with 230V AC and 12V DC (e.g. via a power supply voltage converter).

- If the Temporarily Stationary Equipment is to be located outdoors, it SHOULD be operational in the range of -10 °C to +40 °C and 10% - 90% relative humidity.
- The PC SHOULD have enough CPU power to perform image analysis smoothly. CPU speed MAY be measured with publicly available benchmarks. It is REQUIRED to define such a score;
- Any complete solution element of the Temporarily Stationary Equipment SHOULD NOT EXCEED 23kg if it has to be carried, even if on wheels.

Specific Technical Requirements for Portable Mobile Equipment

- All submitted transactions much be authenticated as coming from a registered and known device and a registered and known user.
- Border Authorities need to define what functionalities are available on the Portable Mobile Equipment, as the equipment MAY support some local watchlist searching capabilities.
- Consideration MUST also be made as to whether the use case functionality available on the equipment involves use cases which generate synchronous or asynchronous transactions.
- Queries to national and European Central Systems which are expected to take longer than the recommendations above, such as identification searches, SHOULD be performed asynchronously via the MS central services. The mobile application SHALL still be usable in another context. When the results of the data query are available, the user SHALL be informed and the previous process MAY continue.
- Mobile equipment SHOULD be operational in the range of -10 °C up to +40 °C
- It is RECOMMENDED that Mobile equipment be at least IP 45 to address accidental dropping and water ingress.
- Portable Mobile equipment SHOULD operate in a "hands free" mode as much as possible.
- It is NOT RECOMMENDED that Portable Mobile Equipment exceed 1.5 kg.
- Mobile equipment MAY have capability to exchange batteries in "on the fly" mode.
- Additional Security measures are MANDATORY:
  - Use of secure elements;
  - Storage of cryptographic keys;
  - Storage of sensitive data;
  - Protection against theft.

Specific Technical Requirements for Digital Mobile equipment and application for travellers

The specific requirements will be addressed in a later version of this document.

Configuration Requirements

Table 3: Mobile Equipment Architecture and Infrastructure Requirements

	Configuration of the Mobile Equipment
Temporarily Stationary Equipment operating as an MBC	Software as per MBC and ability to work as per a fixed MBC on 4G LTE modem as a minimum RECOMMENDED is secure Wi-Fi to national domain OPTIONAL RJ45/Ethernet connection RECOMMENDED is a laptop Rechargeable batteries where minimum operational duration at low temperatures -10 °C up to +10 °C SHOULD be at least 2 hours is OPTIONAL Camera with LED light for facial capture Full page document reader with RFID capability is RECOMMENDED. Document reading capabilities MAY be provided by OCR, software and camera Fingerprint scanner RECOMMENDED is a 4-4-2 fingerprint scanner, minimum is a single finger scanner Additional Security measures are MANDATORY: Use of secure elements Storage of cryptographic keys Storage of sensitive data Protection against theft
Temporarily Stationary Equipment operating as an SSS	Software as per fixed SSS and ability to work on 4G LTE modem as a minimum RECOMMENDED is secure Wi-Fi to national domain OPTIONAL RJ45/Ethernet connection Touch screen is RECOMMENDED Rechargeable batteries where minimum operational duration at low temperatures -10 °C up to +10 °C SHOULD be at least 2 hours is OPTIONAL Camera with LED light for facial capture Full page document reader with RFID capability is RECOMMENDED. Document reading capabilities MAY be provided by OCR, software and camera Fingerprint scanner (integrated or connected through USB cable or Bluetooth/Wi-Fi connection) RECOMMENDED is a 4-4-2 fingerprint scanner, minimum is a single finger scanner. If a single fingerprint scanner is used it is MANDATORY that uniqueness check on the captured fingerprints is made
Portable Mobile Equipment Small	Software with different use cases identifiable on a menu to automatically manage data capture required to meet regulation requirements and support a hands free process as much as possible RECOMMENDED 4G LTE and Wi-Fi Touch screen size RECOMMENDED between 4.5" and 5.5" for handheld solutions (operated by finger or by finger and stylus) Rechargeable batteries operational for 6 hours RECOMMENDED Camera with LED light NFC Reader Software for document OCR MUST support as a minimum a single Fingerprint scanner connected through USB cable or Bluetooth/Wi-Fi connection. Software MUST check uniqueness of all fingerprints captured and perform an automatic quality check.

	Configuration of the Mobile Equipment
Portable Mobile Equipment Medium	Software with different use cases identifiable on a menu to automatically manage data capture required to meet regulation requirements and support a hands free process as much as possible. RECOMMENDED 4G LTE and Wi-Fi. Touch screen size RECOMMENDED between 5.5" and 6" for handheld solutions (operated by finger or by finger and stylus). Rechargeable batteries, operational for 6 hours RECOMMENDED Camera with LED light. Software MUST check the quality of the facial image captured to meet EES requirements (please see Section 2). NFC Reader and Software for document OCR or NFC Reader and integrated MRZ reader. MUST support as a minimum a single Fingerprint scanner connected through USB cable or Bluetooth/Wi-Fi connection, two finger or 4 finger capture OPTIONAL. Software MUST check uniqueness of all fingerprints captured and MUST perform an automatic quality check to meet the requirements of the EES (please see Section 2).
Portable Mobile Equipment Large	Software with different use cases identifiable on a menu to automatically manage data capture required to meet regulation requirement and support a hands free process as much as possible. RECOMMENDED 4G LTE and Wi-Fi. Touch screen size RECOMMENDED between 7" and 10" (operated by finger or by finger and stylus). Rechargeable batteries. Camera with LED light. Software MUST check the quality of the facial image captured to meet EES requirements (please see Section 2). NFC Reader and software for document OCR or NFC Reader and integrated MRZ reader. MUST support as a minimum a single Fingerprint scanner connected through USB cable or Bluetooth/Wi-Fi connection. Two-finger or 4-finger capture OPTIONAL. Software MUST check uniqueness of all fingerprints captured and MUST perform an automatic quality check to meet the requirements of the EES (please see Section 2).
Digital Mobile equipment and application for travellers	Will be addressed at a later date.

3.4.4. Operational functionality for Mobile Equipment

This sub-section addresses specific points related to Mobile Equipment which is covered in Section 2 due to the nature of the solution.

Document authentication

Details of document checks and document authentication processes are described in detail in Section 2. However, when a full page document reader is not used, e.g. normally with Portable Mobile Equipment and Digital Mobile equipment and application for travellers, full functionality for document authentication is not available.

Document authentication during usage of a mobile system under these conditions is RECOMMENDED as follows:

- For MRTD:
  Mobile systems SHALL check the validity of the MRZ and perform a check of the data in the VIZ zone against the data in the MRZ zone. It is RECOMMENDED that a biometric comparison be made between the facial image on the data page and the facial image captured from the traveller.
- For e-MRTD:
  Mobile systems SHALL perform electronic checks which SHALL include checking the authenticity of the document issuer and integrity of the document to ensure that the electronic document has not been cloned. In addition, it is RECOMMENDED that an automatic biometric comparison be made between the facial image on the data page of the travel document and the facial image stored in the document; this can also be further enhanced OPTIONALLY through a comparison with the facial image captured from the physical traveller.

Biometric capture and verification

A mobile system SHALL perform the following operations:

- Biometric enrolment
  - Facial image and fingerprint image capture qualities are specified in Section 2.3;
  - The facial image capture process SHALL ensure that no images displayed on pictures, tablets or smartphones SHALL be acquired. Such Presentation Attacks as well as other attacks with masks SHALL be detected and signalled to the border officer;
  - All fingerprint sensors MUST conform to certification by FBI EBTS Appendix F;
  - The fingerprint sensor SHALL be able to detect presentation attacks such as fake fingerprints. Certified PAD solutions are preferable (i.e. Common Criteria approach);
  - If fingers are captured one at a time, it is MANDATORY to ensure fingerprint uniqueness;
  - OPTIONALLY, the capture software MAY confirm whether the captured fingerprints are from the left hand or the right hand.
- Biometric verification:
  - Facial image and fingerprint image capture quality are specified in Section 2.3;
  - Live facial capture is the same as for Biometric enrolment.
  - Fingerprint image capture is the same as for Biometric enrolment.
  - ISO/IEC 30107-4:2020 includes a profile for Presentation Attack Detection for mobile biometrics.

Equipment requirements

- Cameras mounted in mobile equipment SHOULD be able to capture facial images to be compliant with the EES Regulation. Additional equipment MAY be needed to support the production of uniform and diffused lighting conditions, especially for equipment deployed in the field.
- Fingerprint scanners MAY make LED/LCD indicators visible to travellers to help the fingerprint capture process. The indicators MAY help indicate whether the correct quality capture threshold has been met.

Software requirements

- Mobile systems MUST have native software and libraries for checking the quality of the faces and fingerprints acquired, which could be exchanged with other apps/libraries (eu-LISA USK toolkit).
- The quality assessment of the captured biometrics SHALL be made locally before transmission to central backend systems for enrolment purposes.

Mobile systems MAY have software for performing a local 1:1 verification of the captured face/fingerprint and face/fingerprint obtained from a different source. The parametrisation threshold of the local matching software is specified in Section 2.3.

User interface and guidance

The following guidelines are particularly relevant for Portable Mobile Equipment and Digital Mobile equipment and applications for travellers. It is assumed that the User Interface of the Temporarily Stationary Equipment SHALL be the same as for the Fixed Equipment.

- The User interface SHOULD be operated by finger or/and finger and stylus.
- The User interface SHOULD offer pull down menus for data, which capture standard data that have predefined options.
- The User interface SHOULD perform data quality checks for each screen before moving to the next step in the process. If the quality data check fails, the process cannot move forward and the user SHOULD be informed.
- The officer SHALL assess the quality of the live facial image prior to capture.
- The User interface SHOULD contain all the workflows for each use case to capture the minimum subset of information required by the National and EU systems.
- The User interface SHOULD have workflows already pre-defined for each use case so that the software automatically moves to the next process without the border guard physically having to do anything, and therefore guiding the user through the process;
- The User interface solution SHALL support the user during biometric acquisition, QA result feedback, live-preview, auto/manual capture trigger.
- The User interface MUST be adapted to suit the size of the Mobile Equipment screen when displaying EES identification (alphanumeric or biometric) result lists when there are multiple hits.
- The User interface SHOULD be compliant with design principles underlying mobile OS including:
  - Colours used;
  - Look and feel of the application;
  - Clear navigation;

  - Contextual layout;
  - Good UI performance;
  - Efficient interaction.
- Mobile equipment software and OS features SHALL be compliant with GDPR.
- The software solution SHALL indicate whether a query to a backend system is still pending and that a response is to be expected.
- The device/software SHALL still be usable even if a query is pending (i.e. application context can be switched).

Integration

Table 4 presents the level of Integration REQUIRED by Mobile Systems by category which MUST be managed by a central service.

Table 4: Technical Integration required by Mobile Systems

Management at OS layer	Mobile System Technical Integration		
	Temporarily Stationary Equipment	**Portable Mobile Equipment**	**Digital Mobile equipment and application for travellers**
Remote Data Erasure	Yes	Yes	No
Device Revocation	Yes	Yes	No
Mobile System (Device) Management	Yes	Yes	No
Disk Encryption	Yes	Yes	No
Integration with national PKI to perform Passive and Terminal Authentication	Yes	Yes	No
Location Management	Desirable	Yes	No
Management of Software Application			
Configuration of facial image capture quality	Yes	Yes	Yes if needed
Configuration of fingerprint capture quality	Yes	Yes	No
Configuration of local verification for facial comparison	Yes	Yes	Yes if needed
Configuration of local verification for fingerprint comparison	Yes	Yes	No
Updating of local workflows through a push transaction from the central service	Yes	Yes	Yes
Local logging	Yes	Yes	Yes
Retrieval of logs through an automatic push transaction	Yes	Yes	Yes
Management of devices in the field			
Management of spare parts	Yes	Yes	No
Management of spare devices	Yes	Yes	No
Provision of battery management systems	Yes, if used	Yes	No

It is recognised that working with mobile systems is challenging because the devices are being used in uncontrolled environment.

Quality control and assurance

- All data captured MUST be quality checked locally before a transaction is sent.
- A central monitoring system SHOULD be put in place to manage the mobile equipment deployment.
- The central monitoring system SHOULD be able to produce reports on the operational use and performance metrics of the deployed mobile systems.
- Each device SHOULD have implemented a logging mechanism as defined in Section 2.6, at least for:
  - Check results (document check, biometric checks, background checks);
  - Timestamps of overall process and sub-processes;
  - Device specific data (identifier, software/hardware versions, etc.);
  - User specific data (identifier);
  - The amount of time to transfer data transactions.
- Testing
  - A testing solution replicating each Mobile Equipment solution deployed MUST be maintained both for testing updates to the Mobile Equipment systems and for testing updates to the national and CS-EES workflows and processes.
- Procurement
  - Prior to procurement, it is RECOMMENDED that all hardware claims of the Mobile systems provider be validated:
    - IP rating;
    - Fingerprint sensor;
    - Operational power of the battery (note that the battery last for 6 hours and SHALL continuously work for 6 hours or consider using a Wi-Fi power bank);
    - Weight;
    - Battery swapping functionality, if applicable;
    - Mobile Systems Management.
  - Prior to system acceptance and before operational deployment, it is RECOMMENDED that the Mobile Systems be tested in the field, in a location that is representative of the planned usage site, to validate both the hardware and the software.

3.4.5. Operational and process requirements

The key difference between the deployment of MBC, SSS, e-Gates and ABC at a fixed BCP and the deployment of Mobile Systems is the decision on whether any of the deployed Mobile Systems can be used in an offline mode (data retention on mobile device for processing in back-office).

	Mobile System Technical Integration		
Management at OS layer	**Temporarily Stationary Equipment**	**Portable Mobile Equipment**	**Digital Mobile equipment and application for travellers**
Remote Data Erasure	Yes	Yes	No
Device Revocation	Yes	Yes	No
Mobile System (Device) Management	Yes	Yes	No
Disk Encryption	Yes	Yes	No
Integration with national PKI to perform Passive and Terminal Authentication	Yes	Yes	No
Location Management	Desirable	Yes	No
Management of Software Application			
Configuration of facial image capture quality	Yes	Yes	Yes if needed
Configuration of fingerprint capture quality	Yes	Yes	No
Configuration of local verification for facial comparison	Yes	Yes	Yes if needed
Configuration of local verification for fingerprint comparison	Yes	Yes	No
Updating of local workflows through a push transaction from the central service	Yes	Yes	Yes
Local logging	Yes	Yes	Yes
Retrieval of logs through an automatic push transaction	Yes	Yes	Yes

Temporarily Stationary Equipment

The business process and functionality needed is identical to the Manual Border Control (MBC) process presented in Section 3.1.3. and for the SSS process presented in Section 3.2.4, even though the form factor of the Mobile equipment MAY be different.

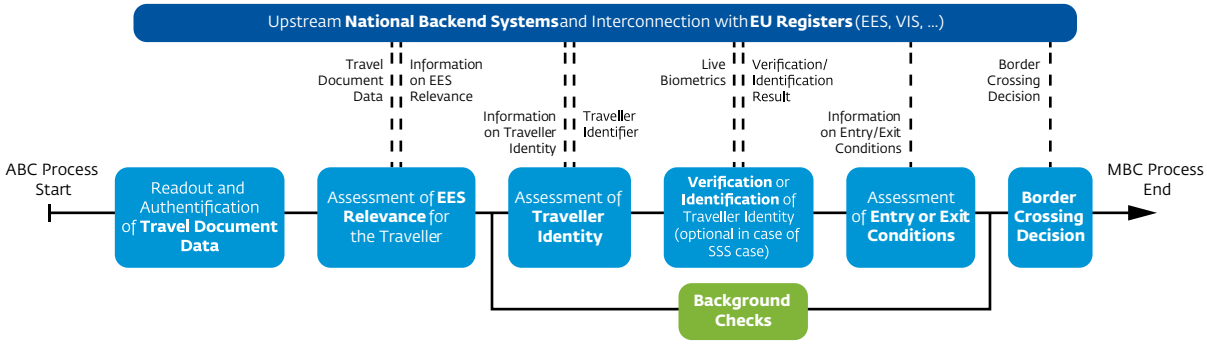

Figure 8: MBC Workflow for Temporarily Stationary Equipment

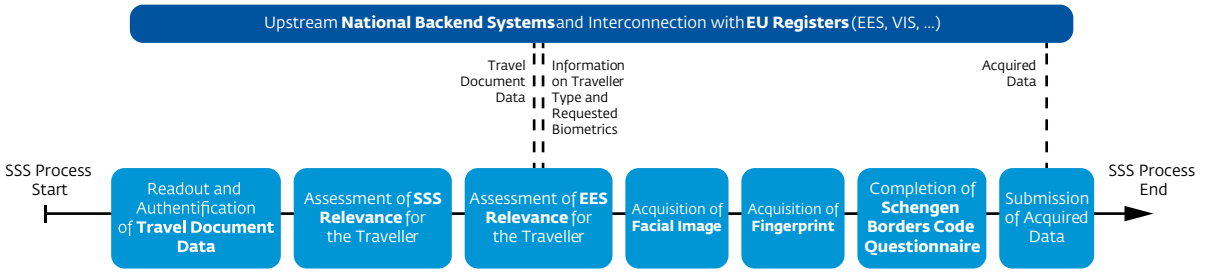

Figure 9: SSS Process Flow

Limitations on performance:

- Response times from the Central System MAY be longer than in the traditional MBC scenario;
- Limitations in the document authentication process if no Full Page Reader is used:
  - The MRZ MUST be scanned by a Swipe Reader (or camera with OCR capabilities) or entered manually;
  - The authenticity of the document MUST be verified visually by the official (supported by external equipment such as a UV lamp, magnifier);
  - After the MRZ is verified, if the document is an e-MRTD, the chip MUST be read via the RFID reader;
- Limitations of the biometric capture process:
  - Positioning of facial image camera (on a stand/tripod or hand-held) MAY be not optimal for full frontal face capture as in the stationary MBC scenario;
  - The correct position of the camera and the traveller to be captured MUST be ensured manually;
  - If a single finger scanner is deployed, a uniqueness check of all fingers to be submitted MUST be performed locally prior to submission of the transaction.

Portable Mobile Equipment:

- Documents' MRZ data MUST be entered into the application, preferably by a camera with OCR capabilities or integrated Swipe Reader; it is NOT RECOMMENDED that the data be entered manually.
- The authenticity of an MRTD MUST be verified visually (supported by external equipment such as a UV lamp, magnifier);
- For an e-MRTD, after the MRZ is verified the chip MUST be read via the RFID reader /NFC module;
- Verified MRZ data MUST be used to perform:
  - For all types of travellers:
    - checks in police information systems such as SIS, SLTD, national databases;
  - For TCNs:
    - alphanumeric checks in the EES and/or VIS;
- Where there is a fingerprint match in the EES or VIS:
  - A facial image MUST be captured to perform a local facial 1:1 verification against the stored image:
    - If the match is positive
      the traveller SHOULD be redirected to a fixed MBC or SSS to capture high-quality biometric features for enrolment into EES;
    - If there is no EES verification/identification
      the traveller SHOULD be redirected to an MBC or SSS to capture the traveller's data for enrolment into EES;
- All EES related tasks (e.g. process hit lists, check assigned visa applications, correct EES calculator) SHALL be carried out and the updated data SHOULD be returned to the CS-EES;
  - The Process MUST be concluded by submitting the final decision of the official:
    - Grant entry or exit, refuse entry or exit, redirect to Second Line inspection.

Digital Mobile equipment and application for travellers:

Step 1: Self-service pre-processing

- Traveller MUST enter document data (by camera with OCR capabilities or manually) into the APP;
- Traveller MAY enter document data page by performing a photo scan;
- Traveller MAY enter chip data by reading it via the NFC module, if carrying an e-MRTD;
- Traveller MAY capture his/her selfie. It is RECOMMENDED that a liveness check be integrated into the capture process;
- The APP MAY perform:
  - a local comparison of the captured facial image against the image from the data page scan or the digital image in the chip; or
  - a central comparison of the captured facial image against the image from the data page scan or the digital image in the chip;
- Traveller SHOULD perform a self-declaration on the purpose of his/her intended stay and means of subsistence, and answer any additional questions which the MS requires a response to;
- The APP SHALL generate a QR code in a specified format that can be read by the National Infrastructure at the intended BCP:

- The QR code MAY encode the required traveller data; or
- The QR code MAY point to a central service where the data has been stored and which makes it available.

Step 2: Process at the BCP

- At an MBC:
  - Traveller SHALL provide the QR code for data transfer and processing when requested.
- At an SSS:
  - The traveller will provide the QR code after reading of his/her MRTD/e-MRTD for data transfer and processing;
  - The traveller's biometric data will be captured:
    - OPTIONALLY, the facial images of the e-MRTD, the facial image from the QR code and the live captured facial image of the traveller can be compared;
    - The traveller MUST validate the submission of his/her responses to the questions posed prior to terminating the process at the SSS.

Enrolment

The requirements for the enrolment of traveller data for the EES are the same for all kinds of border control scenarios. Because mobile systems are mainly in use under varying environmental conditions (e.g. indoor with artificial light, outdoor – sunlight, outdoor – cloudy), the capturing of high quality facial images in particular is challenging. Other specifics of mobile systems may be the reduced capabilities of biometric capture devices (e.g. small form factor, no integrated user feedback).

Depending on the category of the mobile system, the enrolment process has different characteristics.

Temporarily Stationary Equipment:

- Enrolment of facial image
  - The face capture system (camera incl. software) SHALL provide the same functionality as in the MBC process (see Section 2.3.1).
  - Usually the face camera is temporarily mounted on a stand or tripod.
  - The mobile systems SHALL allow the capture of a facial image person in automatic mode (auto face detection) and manual mode.
  - A quality evaluation SHALL be performed requirements (see Section 2.3.1).
  - At least the official SHALL assess the acquired facial image prior to enrolment.
- Enrolment of fingerprint images
  - The fingerprint capture system (scanner incl. software) SHALL provide the same functionality as in the MBC process (see Section 2.3.2).
  - It is RECOMMENDED that this category of mobile system is equipped with a four-fingerprint scanner.
  - The mobile system SHALL capture fingerprints in automatic mode (auto-capture) or manual mode (as a fallback).
  - A quality evaluation SHALL be performed (see Section 2.3.2).

Portable Mobile Equipment:

- Enrolment of facial image
  Capability of performing EES enrolment scenario and EES pre-enrolment scenario with Portable Mobile Equipment is limited; however, when there is no other possibility to perform this task it is RECOMMENDED that biometrics captured with such a device meet the same quality requirements for facial images (see Section 2.3.1).
- Enrolment of fingerprint images
  Capability of performing EES enrolment scenario and EES pre-enrolment scenario with Portable Mobile Equipment is limited; however, when there is no other possibility to perform such a task it is RECOMMENDED that biometrics captured with such a device meet the same quality requirement for fingerprint images (see Section 2.3.2).

Digital Mobile equipment and application for travellers:
Biometric data captured on a mobile device of the traveller SHALL NOT be used for enrolment into the EES.

Verification
Mobile System Equipment MAY support 1:1 verification of live captured biometric features (face or fingerprints) against biometric features from other sources (mainly DG2/DG3 of the e-MRTD). The 1:1 verification MAY be performed centrally (MS domain) or locally on the device.

Temporarily Stationary Equipment or Portable Mobile Equipment SHOULD be used to provide live captured biometric features (face or fingerprints) to the EES for the verification of a selected EES or VIS dossier. The verification MUST be processed on a Central System (on EU level).

Handling exceptions

Temporarily Stationary Equipment
It is assumed that the handling of exceptions will be similar if not identical to that of an MBC or an SSS.

Portable Mobile Equipment:
It is RECOMMNDED that equipment be used offline for no more than two hours and that the data captured and stored on the device during offline use be submitted as soon as network connectivity is available.

Fallback
An MS SHOULD define procedures to act as fallback processes for each category of the Mobile System if the deployment fails.

4. References

4.1. EU references

Table 5: List of EU References

[C(2019) 1230]	"Commission Implementing Decision laying down the specifications and conditions for the web service of the Entry/Exit System (EES) including specific provisions for the protection of the data where provided by or to carriers" European Commission, 25 February 2019
[C(2019) 1230 A]	Annex to the "Commission Implementing Decision laying down the specifications and conditions for the web service of the Entry/Exit System (EES) including specific provisions for the protection of the data where provided by or to carriers" European Commission, 25 February 2019
[C(2019) 1240]	"Commission Implementing Decision laying down the specifications and conditions for the data repository of the Entry/Exit System (EES)" European Commission, 25 February 2019
[C(2019) 1260]	"Commission Implementing Decision laying down performance requirements of the Entry/ Exit System (EES)" European Commission, 25 February 2019
[C(2019) 1260 A]	Annex to the "Commission Implementing Decision laying down performance requirements of the Entry/Exit System (EES)" European Commission, 25 February 2019
[C(2019) 1270]	"Commission Implementing Decision laying down measures for the establishment and the high level design of interoperability between the Entry/Exit System (EES) and the Visa Information System (VIS)" European Commission, 25 February 2019
[C(2019) 1270 A]	Annex to the "Commission Implementing Decision laying down measures for the establishment and the high level design of interoperability between the Entry/Exit System (EES) and the Visa Information System (VIS)" European Commission, 25 February 2019
[C(2019) 7131 A]	Annex to the "Commission Recommendation establishing a common Practical Handbook for Border Guards" to be used by Member States' competent authorities when carrying out the border control of persons and replacing Commission Recommendation C(2006) 5186 of 6 November 2006" European Commission, 8 October 2019
[C(2018) 7774]	"Commission Implementing Decision laying down the technical specifications regarding the standards for security features and biometrics in passports and travel documents issued by Member States and repealing Decision C(2006) 2909 and C(2008) 8657" European Commission, 30 November 2018
[C(2018) 7774 A]	Annex to the "Commission Implementing Decision C(2018) 7774 final laying down the technical specifications regarding the standards for security features and biometrics in passports and travel documents issued by Member States and repealing Decisions C(2006) 2909 and C(2008) 8657" European Commission, 30 November 2018
[CEN/TC 224/ WG 18]	TC 224 WI (E) TR European Enrolment Guide draft v.6.1: "European Enrolment Guide for Biometric ID Documents" European Committee for Standardization, 29 October 2019
[EL_Draft]	"Workflow Engine Draft v.0.12" eu-LISA, 11 July 2018
[EL-03-19-726-EN-N]	Entry/Exit System (EES) Working Group on ICT Solutions for External Borders (sea/land) Report" eu-LISA, 26 March 2019
[EL-ICD]	EES - Interface Control Document eu-LISA, v.04.00.00, 16 December 2019
[EL-DCP]	EES - MS Data Centre Preparation eu-LISA, v.01.070, 02 October 2019
[EU 2019/326]	"Commission Implementing Decision (EU) 2019/326 laying down measures for entering the data in the Entry/Exit System (EES)" European Commission, 25 February 2019
[EU 2019/327]	"Commission Implementing Decision (EU) 2019/327 laying down measures for accessing the data in the Entry/Exit System (EES)" European Commission, 25 February 2019
[EU 2019/328]	"Commission Implementing Decision (EU) 2019/328 laying down measures for keeping and accessing the logs in the Entry/Exit System (EES)" European Commission, 25 February 2019

[EU 2019/329]	"Commission Implementing Decision (EU) 2019/329 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System" European Commission, 25 February 2019
[EU 2019/817]	Regulation (EU) 2019/817 of The European Parliament and of The Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA
[EU 2019/818]	Regulation (EU) 2019/818 of The European Parliament and of The Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816
[EU 2016/399]	Regulation (EU) 2016/399 of the European Parliament and of the Council on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code)" European Parliament and Council of the European Union, 23 March 2016
[EU 2003/693]	Regulation (EC) /2003/693
[EU 2019/679]	Regulation (EU) 2019/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" European Parliament and Council of the European Union, 27 April 2016
[EU 2018/1547]	"Commission Implementing Decision (EU) 2018/1547 laying down the specifications for the connection of the central access points to the Entry/Exit System (EES) and for a technical solution to facilitate the collection of data by Member States for the purpose of generating statistics on the access to the EES data for law enforcement purposes" European Commission, 15 October 2018
[EU 2018/1548]	"Commission Implementing Decision (EU) 2018/1548 laying down measures for the establishment of the list of persons identified as overstayers in the Exit-Entry System (EES) and the procedure to make that list available to Member States" European Commission, 15 October 2018
[EU 2018/1860]	Regulation 2017/2225 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals
[EU 2017/2225]	Regulation 2017/2225 of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System" European Parliament and Council of the European Union. 20 November 2017
[EU 2017/2226]	Regulation (EU) 2017/2226 of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011" European Parliament and Council of the European Union, 30 November 2017
[EU 2017/1724]	Regulation (EU) 2017/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012
[EU 2014/30]	EMC Directive
[FRONTEX 2014]	Good Practices for the practical implementation of the Visa Information System at EU borders" European Border and Coast Guard Agency, September 2014
[FRONTEX 2015]	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX): "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems", 2015; "Best Practice Operational Guidelines for Automated Border Control (ABC) Systems", 2015
[FRONTEX 2019]	Vulnerability Assessment and Testing for Automated Border Control (ABC) Systems Course Manual" European Border and Coast Guard Agency, 2019
[PRADO]	The General Secretariat of the Council: PRADO - Public Register of Authentic travel and identity Documents Online, http://www.consilium.europa.eu/prado/en/prado-start-page.html" European Council and Council of the European Union

4.2. International references

Table 6: List of International References

[ICAO 9303]	Machine Readable Travel Documents, Parts 1 – 12, 7th Edition,International Civil Aviation Organization (ICAO), 2015
[ICAO 2018]	Best Practice Guidelines for Optical Machine Authentication, Part 1, Version 1.2, International Civil Aviation Organization (ICAO), 2018
[ISO/IEC 2382-37]	ISO/IEC 2382-37:2017 Information technology — Vocabulary – Part 37: Biometrics, International Organization for Standardization (ISO), 2017
[ISO/IEC 10918]	JPG
[ISO/IEC 15444-1]	JPEG 2000 (ISO/IEC 15444-1 image compression standard
[ISO/IEC 19794-4:2011]	Information technology — Biometric data interchange formats — Part 4: Finger image data, International Organization for Standardization (ISO), December 2011
[ISO/IEC 19794-5:2011]	Information technology — Biometric data interchange formats — Part 5: Face image data, International Organization for Standardization (ISO), November 2011
[ISO/IEC 19795:2006]	Information technology — Biometric performance testing and reporting. International Organization for Standardization (ISO), June 2005
[ISO/IEC 30107:2016]	Information technology — Biometric presentation attack detection. International Organization for Standardization (ISO), June 2005
[ISO/IEC 30116]	ISO/IEC 30116:2016 Information technology — Automatic identification and data capture techniques — Optical Character Recognition (OCR) quality testing. Edition 1, International Organization for Standardization, October 2016
[ISO1831]	International Organization for Standardization (ISO) 1831: Printing specifications for optical character recognition, Edition 1, 1980
[NIST_NFIQ]	NIST Fingerprint Image Quality, open-source framework and reference implementation of fingerprint quality assessment algorithm, http://www.nist.gov/itl/iad/ig/development_nfiq_2.cfm, National Institute of Standards and Technology (NIST), February 2011
[NISTIR 8280]	Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 19 December 2019

4.3. National references from Member States

Table 7: List of National References from Member States

[BSI-TR03110]	Technical Guideline TR-03110: "Advanced Security Mechanisms for Machine Readable Travel Documents", Federal Office for Information Security (BSI), Germany
[BSI-TR03121]	Technical Guideline TR-03121: "Biometrics in Public Sector Applications", Federal Office for Information Security (BSI), Germany, www.bsi.bund.de/en/TRBiometrics
[BSI-TR03122]	Technical Guideline TR-03122: "Conformance Test Specification for BSI TR-03121 Biometrics for Public Sector Applications", Federal Office for Information Security (BSI), Germany
[BSI-TR03135]	Technical Guideline TR-03135: "Machine Authentication of MRTDs for Public Sector Applications", Federal Office for Information Security (BSI), Germany, www.bsi.bund.de/en/TRDocCheck
[BSI-TR03156]	Technical Guideline TR-03156: "Public Sector Identity Management in Conjunction with European Registers", Federal Office for Information Security (BSI), Germany, www.bsi.bund.de/en/TRIDM

4.4. References for figures

Table 8: List of References for Figures

Figure 2: Workflow for checking e-MRTDs	German Federal Office for Information Security (BSI)
Figure 4: Vulnerability points in a biometric system	Dunstone, T. and Yager N. (2009): Biometric System and Data Analysis, Springer, New York
Figure 5: Generic EES Operational Process	German Federal Office for Information Security (BSI) and the German Federal Police
Figure 6: SSS Process Flow	German Federal Office for Information Security (BSI) and the German Federal Police
Figure 7: Process Flow	German Federal Office for Information Security (BSI) and the German Federal Police
Figure 8: MBC Workflow for Temporarily Stationary Equipment	German Federal Office for Information Security (BSI) and the German Federal Police
Figure 9: SSS Process Flow	German Federal Office for Information Security (BSI) and the German Federal Police

5. Annex

5.1. Definitions

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 or cloned, by means of a challenge-response protocol between the inspection system and the e-MRTD's chip. See also 'Chip Authentication (CA)'.

Alphanumeric data - Data represented by letters, digits, special characters, spaces and punctuation marks.

Alteration detection - Detects features characteristic of attempts to alter a biometric feature [ISO/IEC 30107- 1:2016].

Artefact - Artificial object or representation presenting a copy of biometric characteristics or synthetic bio-metric patterns [ISO/IEC 30107-1:2016]. See also 'Presentation Attack Instrument (PAI)'.

Artefact species - Artefacts based on a common medium and production methodology but with different biometric characteristic references.

Attack vector - A path or means by which an attacker can gain the ability to exercise malicious intent.

Authentication - The process of comparing sets of data to establish the authenticity of data concerning an identity (many-to-one check).

Authorisation - The process of deciding based upon sets of data to establish whether a person is allowed to pass the border (yes-or-no decision).

Automated Border Control (ABC) System - A system which allows for an automated border crossing, composed of a self-service system (SSS) and an e-Gate.

Basic Access Control - 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)'.

Binding corporate rules - Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Biometric capture - Obtain and record, in a retrievable form, signal(s) of biometric characteristic(s) directly from individual(s), or from representation(s) of biometric characteristic(s) [ISO/IEC 2382-37:2017].

Biometric data (EES Regulation) - Fingerprint data and facial image.

Biometric feature - Numbers or labels extracted from biometric samples and used for comparison [ISO/IEC 2382-37:2017]. See also 'Biometric data' and 'Biometric feature'.

Biometric fraud - The abuse of metrics related to human characteristics for wrongful or criminal deception intended to result in financial or personal gain.

Biometric identification - Process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single individual [ISO/IEC 2382-37:2017].

Biometric probe - Biometric query. Biometric sample or biometric feature set input to an algorithm for use as the subject of biometric comparison to a biometric reference(s) [ISO/IEC 2382-37:2017]. See also 'Biometric data' and 'Biometric feature'.

Biometric property - Descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means [ISO/IEC 2382-37:2017]. See also 'Biometric data'.

Biometric recognition/ biometrics - Automated recognition of individuals based on their biological and behavioural characteristics [ISO/IEC 2382-37:2017]. See also 'Biometric system'.

Biometric reference - One or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison [ISO/IEC 2382-37:2017].

Biometric sample - Analog or digital representation of biometric characteristics prior to biometric feature extraction [ISO/IEC 2382-37:2017].

Biometric system - System for the purpose of the biometric recognition of individuals based on their behavioural and biological characteristics [ISO/IEC 2382-37:2017].

Biometric template - Reference biometric feature set. Set of stored biometric features comparable directly to probe biometric features [ISO/IEC 2382-37:2017]. See also 'Biometric feature'.

Biometric verification - Process of confirming a biometric claim through biometric comparison [ISO/IEC 2382- 37:2012].

Biometric vulnerability - A weakness that allows an attacker to reduce a system's security posture that may result in unauthorised users being falsely accepted.

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.

Border control - The activity carried out at a border, in accordance with and for the purposes of this Regulation, in response exclusively to an intention to cross or the act of crossing that border, regardless of any other consideration, consisting of border checks and border surveillance.

Border crossing point - 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 out, in accordance with this Regulation and national law, border control tasks.

Border surveillance - The surveillance of borders between border crossing points and the surveillance of border crossing points outside the fixed opening hours, in order to prevent persons from circumventing border checks.

Candidate list - A list of pair-wise biometrics data comparisons that that are in an ascending order and that create a similarity score between the reference template and the verification sample features. A candidate list is produced only in an identification process.

Carrier - Any natural or legal person whose profession it is to provide transport of persons.

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. See also 'Biometric data'.

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

Cloning - Duplication or copying of an item such as a passport chip.

Collusion - Cooperation or conspiracy in order to deceive others.

Comparison process - Creates a similarity score between the reference template and the verification sample features.

Confirmation of the authenticity and integrity of the chip data - the process by which it is verified, through the use of certificates, that the data on the electronic storage medium (chip) originate from the issuing authority and that they have not been changed.

Consent of the data subject - Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Controller - The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Cross-border processing - (a) Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) Processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Cruise ship - A ship which follows a given itinerary in accordance with a predetermined programme, which includes a programme of tourist activities in the various ports, and which normally neither takes travellers on nor allows travellers to disembark during the voyage.

Data concerning personal health - Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

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.

Decision policy - The decision policy uses business rules to convert the match results into a final acceptance or rejection.

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.

Defence in depth - The coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defence system than to penetrate a single barrier.

Denial of service (DoS) attacks - An attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users.

Designated authority - An authority designated by a Member State pursuant to Article 29 as responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

Detection and identification rate - The rate at which individuals who are in a database cause a system alarm and are properly identified in an open-set identification (watch list) application.

Document Signer (DS) - A DS is a certificate that contains the information required to verify the digital signature on an e-Passport. In contrast to CSCA certificates, which remain relatively static due to their longer validity period, a large number of DS certificates will be created over time. The root certificates (CSCA certificates) are used to sign the DS certificates used by manufacturers for production of passports or ID cards.

EES data - All data stored in the EES Central System in accordance with Article 14 and Articles 16 to 20.

e-Gate (eu-LISA) - Infrastructure operated by electronic means where an external border or an internal border where controls have not yet been lifted is actually crossed.

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.

Enrolment database - A database of enrolled biometrics.

Enterprise - A natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in economic activity.

e-Passport or e-MRTD - A machine readable passport (MRP) containing a Contactless Integrated Circuit (IC) chip which stores 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 and 9.

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.

eu-LISA - The European Agency for the operational management of large-scale information systems in the area of freedom, security and justice established by Regulation (EU) No. 1077/2011.

Extended Access Control (EAC) - Protection mechanism to access 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.

External borders (SBC) - The Member States' land borders, including river and lake borders, sea borders and their airports, river ports, seaports and lake ports, provided that they are not internal borders.

Facial image - Digital images of the face.

Failure to Enrol Rate (FTER) - The proportion of enrolments/registrations with insufficient quality of the biometric enrolment.

False Accept Rate (FAR) - The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The false accept rate may be estimated as FAR = NFA/NIIA or FAR = NFA/NIVA where FAR is the false accept 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 alarm rate - The percentage of times an alarm or an alert is incorrectly sounded on an individual who is not in the biometric system's database (the system alarms on Frank when Frank is not in the database), or an alarm is sounded but the wrong person is identified (the system alarms on John when John is in the database, but the system thinks John is Steve).

False match - Comparison decision of "match" for a biometric probe and a biometric reference that are from different biometric capture subjects [ISO/IEC 2382-37:2017].

False Matching Rate (FMR) - The proportion of impostor attempts that are falsely declared to match a template of another object (a person's biometric template).

False Negative Identification Rate (FNIR) - The proportion of missed matches during a biometric search even though the traveller's biometric data were registered.

False Non-Match(ing) Rate (FNMR) - The proportion of genuine attempts that are falsely declared not to match a template of the same object.

False Positive Identification Rate (FPIR) - The proportion of returned matches during a biometric search which do not belong to the checked traveller.

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 reject rate may be estimated as follows: FRR = NFR/NEIA or FRR = NFR/NEVA where FRR is the

false reject 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 reject rate normally excludes 'failure to acquire' error.

Feature extraction - The process by which key features of the sample are selected or enhanced.

Filament - The fibres of the iris.

Filing system - Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Fingerprint data - The data relating to the four fingerprints of the index, middle finger, ring finger and little finger from the right hand where present, and otherwise from the left hand.

Genetic data - Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Group of undertakings - A controlling undertaking and its controlled undertakings.

Identification - The process of determining a person's identity through a database search against multiple sets of data (one-to-many check).

Identity claim - A statement by an individual about who they are. In a border context this is generally done by the presentation of a passport as a token.

Immigration authority - The competent authority responsible, in accordance with national law, for one or more of the following:

(a) checking within the territory of the MS whether the conditions for entry to, or stay on, the territory of the MS are fulfilled;

(b) examining the conditions for, and taking decisions related to, the residence of third-country nationals on the territory of the MS insofar as that authority does not constitute a 'determining authority' as defined in point (f) of Article 2 of Directive 2013/32/EU of the European Parliament and of the Council (1), and, where relevant, providing advice in accordance with Council Regulation (EC) No 377/2004 (2);

(c) the return of third-country nationals to a third country of origin or transit.

Impostor – A subversive biometric capture subject who attempts to be matched to someone else's biometric reference [ISO/IEC 2382-37:2017].

Information society service - A service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council: 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

Integrated Two-Step Process - One of the possible typologies 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 typology is invariably implemented by using a mantrap e-Gate.

Internal borders

(a) the common land borders, including river and lake borders, of the Member States;
(b) the airports of the MS for internal flights;
(c) sea, river and lake ports of the MS for regular internal ferry connections.

Internal flights - Any flight exclusively to or from the territories of the MS and not landing on the territory of a third country.

International organisation - An organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Law enforcement - The prevention, detection or investigation of terrorist offences or other serious criminal offences.

Liveness detection - Measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture. Liveness detection methods are a subset of presentation attack detection methods [ISO/IEC 30107-1:2016].

Liveness - Quality or state of being alive made evident by anatomical characteristics, involuntary reactions or physiological functions, or voluntary reactions or subject behaviours [ISO/IEC 30107-1:2016].

Machine Readable Travel Document (MRTD) - An 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.

Machine Readable Zone (MRZ) - Fixed dimensional area located on the MRTD, containing mandatory and optional data formatted for machine reading using OCR methods.

Main establishment

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.

Master List (ML) - A signed list that contains CSCA certificates and CSCA link certificates which are authorised by a certain ML issuing authority. Certificates on a Master Lists are "trusted certificates" (trusted by the ML issuing authority) which e.g. can be used during border control processes.

Match - Refers to the process of the degree of match (usually in the form of a match score) between two biometric signatures, one usually collected at the biometric enrolment stage and the other collected at the biometric verification or identification stage.

Match Comparison - Decision stating that the biometric probe(s) and the biometric reference are from the same source [ISO/IEC 2382-37:2017].

Member State - A country that is a member of the European Union. Within the context of the present Trainer's Manual, the term also applies to those countries that, not being EU members, take part in the Schengen area.

Member State responsible - The Member State which has entered data in the EES.

Mitigation strategies - Options or actions to reduce risk.

Modality - A type or "mode" of biometric (e.g. fingerprints).

Mode - Combination of a biometric characteristic type, a sensor type and a processing method [ISO/IEC 2382- 37:2012].

Multi-modal - Multiple in at least two out of three constituents of a mode in a single biometric system [ISO/IEC 2382-37:2017].

National short-stay visa - An authorisation issued by a Member State with a view to: transit through or an intended stay on the territory of the MS of a duration of no more than three months in any six-month period from the date of first entry onto the territory of the MS.

Near-Infrared Range (NIR) - A specific wavelength (type) of light.

Offshore worker - A person working on an offshore installation located in the territorial waters or in an area of exclusive maritime economic exploitation of the MS, as defined under the international law of the sea, and who returns regularly by sea or air to the territory of the MS.

One-Step Process - One of the possible typologies of ABC systems. An ABC system designed as a one-step process combines the verification of the traveller and the traveller's passage through the border. This design allows the traveller to complete the whole transaction in one single process. It usually takes the form of a mantrap e-Gate.

Operator - The border guard officer responsible for the remote monitoring and control of the ABC system. The tasks performed by the operator typically include:

(a) monitor the user interface of the application;
(b) react upon any notification given by the application;
(c) manage exceptions and make decisions about them;
(d) communicate with the assisting personnel for the handling of exceptions at the e-Gates;
(e) monitor and profile travellers queuing in the ABC line and using the e-Gates, looking for suspicious behaviour in travellers; and
(f) communicate with the border guard officers responsible for Second Line checks whenever their service is needed.

Overstayer - A third-country national who does not fulfil or no longer fulfils the conditions relating to the duration of his or her authorised short stay on the territory of the MS.

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

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.

Personal data - Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Persons enjoying the right of free movement under Union law -
(a) Union citizens within the meaning of Article 20(1) TFEU, 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 (21) applies;

(b) third-country nationals and their family members, whatever their nationality, who, under agreements between the Union and its MS, on the one hand, and those third countries, on the other hand, enjoy rights of free movement equivalent to those of Union citizens.

Persons for whom an alert has been issued for the purposes of refusing entry - Any third-country national for whom an alert has been issued in the Schengen Information System (SIS) in accordance with and for the purposes laid down in Articles 24 and 26 of Regulation (EC) No 1987/2006 of the European Parliament and of the Council (22).

Pleasure boating - The use of pleasure boats for sporting or tourism purposes.

Presentation - The provision of a biometric for capture.

Presentation attack - Spoofing (deprecated). Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system. A presentation attack can be implemented through a number of methods, e.g. artefact, mutilations, replay, etc. Presentation attacks may have a number of goals, e.g. impersonation or not being recognised. Biometric systems may not be able to differentiate between biometric presentation attacks with the goal of interfering with the systems operation and non-conformant presentations. [ISO/IEC 30107-1:2016].

Presentation Attack Detection (PAD) - Automated determination of a presentation attack. PAD cannot infer the subject's intent. In fact it may be impossible to derive that difference from the data capture process or acquired sample [ISO/IEC 30107-1:2016].

Presentation Attack Instrument (PAI) - Biometric characteristic or object used in a presentation attack. The set of PAI includes artefacts but would also include lifeless biometric characteristics (i.e. stemming from dead bodies) or altered biometric characteristics (e.g. altered fingerprints) that are used in an attack [ISO/IEC 30107-1:2016].

Processing - Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor - A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Pseudonymisation - The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of

additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

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

Quality control - A process of ensuring sufficient quality for biometric captures/enrolments.

Recipient - A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law SHALL NOT be regarded as recipients; the processing of those data by those public authorities SHALL be in compliance with the applicable data protection rules according to the purposes of the processing.

Regular internal ferry connection - Any ferry connection between the same two or more ports situated on the territory of the MS, not calling at any ports situated outside the territory of the MS, and consisting of the transport of travellers and vehicles according to a published timetable.

Relevant and reasoned objection - An objection to a draft decision as to whether there is an infringement of the GDPR Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union.

Representative - A natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.

Residence permit -

(a) all residence permits issued by the MS according to the uniform format laid down by Council Regulation (EC) No 1030/2002 (23) and residence cards issued in accordance with Directive 2004/38/EC;

(b) all other documents issued by a Member State to third-country nationals authorising a stay on its territory that have been the subject of a notification and subsequent publication in accordance with Article 39, with the exception of:

(i) temporary permits issued pending examination of a first application for a residence permit as referred to in point (a) or an application for asylum; and

(ii) visas issued by the MS in the uniform format laid down by Council Regulation (EC) No. 1683/95 (24).

Restriction of processing - Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or other-

wise making available, alignment or combination, restriction, erasure or destruction; 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Risk management - The forecasting and evaluation of risks together with the identification of treatments to avoid or minimise their impact.

Risk management plan - A document that outlines risks and treatments, and defines responses to issues.

Schengen area - An area without internal border controls encompassing 26 European countries, including all EU MS except Bulgaria, Croatia, Cyprus, Ireland, Romania, 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 persons are checked (the First Line).

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

Self-Service System (SSS) (eu-LISA Workflow Engine) - an automated system which performs all or some of the border checks that are applicable to a person and which may be used for pre-enrolling data in the EES.

Serious criminal offence - An offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of Framework Decision 2002/584/JHA, if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.

Service Level Agreements (SLAs) - A contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider.

Shared border crossing point - Any border crossing point situated either on the territory of a Member State or on the territory of a third country, at which Member State border guards and third-country border guards carry out exit and entry checks one after another in accordance with their national law and pursuant to a bilateral agreement.

Short stay - Stays on the territory of the MS of a duration of no more than 90 days in any 180-day period as referred to in Article 6(1) of Regulation (EU) 2016/399.

Short stay visa - An authorisation issued by a Member State with a view to: transit through or an intended stay on the territory of the MS of a duration of no more than three months in any six-month period from the date of first entry onto the territory of the MS.

Similarity score - Distance score. Comparison score that increases with similarity (ISO/IEC 2382-37:2017).

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

Standard Operating Procedure (SOP) - A set of step-by-step instructions compiled by an organisation to help workers carry out routine operations.

Supervisory authority - An independent public authority which is established by a Member State pursuant to Article 51.

Supervisory authority concerned - A supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority.

System audit - An evaluation of a system and the components which it comprises.

System commissioning - Bringing a system into operation.

Template - A digital reference of distinct characteristics that have been extracted from a sample. Templates are used during the biometric verification process.

Terminal authentication - Mechanism ensuring that only authorised inspection system terminals get access to sensitive chip data. Part of the EAC protocol. See 'Extended Access Control'.

Terrorist offence - An offence under national law which corresponds or is equivalent to one of the offences referred to in Directive (EU) 2017/541.

Third party - A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Third country national - Any person who is not a citizen of the Union within the meaning of Article 20(1) TFEU, with the exception of persons who enjoy the right of free movement equivalent to that of Union citizens under agreements between the Union and its MS, on the one hand, and third countries, on the other.

Threat agent(s) - An individual, group or method that can manifest a threat to the security of a facility, operation, or system by exploiting a vulnerability.

Threat to public health - Any disease with epidemic potential as defined by the International Health Regulations of the World Health Organization and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the MS.

Threshold process - Compares the similarity score with a defined threshold.

Traveller Data – Surname (family name), first name or names (given name), date of birth, nationality or nationalities, sex, type and number of travel document or documents and the three letter code of the issuing country (or the travel document or documents), date of expiry of the validity of the travel document or documents (Article 16(1) of EU 2017/2226); visa data (Article 16(2) of EU 2017/2226); biometric data (facial image and fingerprint data, Article 17(1) of EU 2017/2226).

Travel document - A passport or other equivalent document entitling the holder to cross the external borders and to which a visa may be affixed.

True Presentation Attack Detection Rate - The proportion of attack presentations correctly classified.

True Presentation Attack Non-Detection Rate - The proportion of non-attack presentations correctly classified.

Typology - The way in which the constituent parts of a system are interrelated and/or arranged.

User (of a biometric system) - Person or organisation interacting in any way with a biometric system [ISO/IEC 2382-37:2017].

Verification - The process of comparing sets of data to establish the validity of a claimed identity (one-to-one check).

Verification attempt - Biometric claim and capture attempt(s) that together provide the inputs for comparison(s) [ISO/IEC 2382-37:2017].

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'.

Verification rate - The rate at which legitimate users are correctly verified.

Visa authorities - Authorities which in each Member State are responsible for examining and for taking decisions on visa applications or for decisions whether to annul, revoke or extend visas, including the central visa authorities and the authorities responsible for issuing visas at the border in accordance with Council Regulation (EC) No 415/2003 of 27 February 2003 on the issue of visas at the border, including the issue of such visas to seamen in transit.

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

Vulnerability - A weakness in the ABC system that may 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'.

Acronyms and abbreviations

AA	Active Authentication
ABC	Automated Border Control
ANSI	American National Standards Institute
API	Advanced Passenger Information
BAC	Basic Access Control
BCMW	Border Control MiddleWare
BCP	Border Crossing Point
BG	Border Guard
BMP	Bitmap Image File (image file format)
BPOL	Federal Police (Germany)
BSI	Federal Office for Information Security (Germany)
BVA	Federal Office of Administration (Germany)
CA	Chip Authentication
CAN	Card Access Number
CBD	Capacity Building Division
CCTV	Closed-Circuit Television
CED	Centre for Excellence for Combatting Document Fraud
CIR	Common Identity Repository
COTS	Commercial off-the-shelf
CPU	Central Processing Unit
CRL	Certificate Revocation List
CS-EES	EES Central System (under the control of eu-LISA)
CSCA	Country Signing Certification Authority
DC	Direct Current
DCP	Data Centre Preparation
DET	Detection Error Tradeoff
DFL	Defect List
DG	Data Group (readable data stored in the passport chip memory)
DoS	Denial of Service
dpi	Dots Per Inch
DPO	Data Protection Officer
DS	Document Signer
e-Gate	Electronic Gate (automated self-service barrier)
EAC	Extended Access Control
EBCGA	European Border and Coast Guard Agency
EBTS	Electronic Biometric Transmission Specification
ECRET	European Centre for Returns
ECRIS	European Criminal Records Information System
EDP	European Data Protection
EEA	European Economic Area
EES	Entry/Exit System
EMC	Electromagnetic Compatibility Directive
e-MRTD	electronic Machine Readable Travel Document
EN	European Standard
ETIAS	European Travel Information and Authorisation System
EU	European Union

eu-LISA	The European Agency for Large-Scale IT Systems in the area of liberty, security and justice
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FI	Facial Image
FMR	False Match Rate
FNIR	False Negative Identification Rate
FNMR	False Non-Match Rate
FOM	Freedom of Movement travellers
FPIR	False Positive Identification Rate
FP	Fingerprint
FRR	False Reject Rate
FTD	Facilitated Transit Document
FTER	Failure to Enrol Rate
GDPR	General Data Protection Regulation
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HTML	Hypertext Markup Language
ICAO	International Civil Aviation Organization
ICD	Interface Control Document
ID	Identity Document
IEC	International Electrotechnical Commission
INTERPOL	International Criminal Police Organization
iOS	Apple Inc. mobile operating system
IR	Infrared electromagnetic radiation
ISBN	International Standard Book Number
ISO	International Standards Organization
ITL	Information Technology Laboratory
JPEG	Joint Photographic Experts Group (compression method for digital images)
JRC	Joint Research Centre
LED	Light-emitting diode
LTE	Long-Term Evolution
MBC	Manual Border Control
MEMS	Micro-Electro-Mechanical Systems
MID	Multiple Identity Detector
MRTD	Machine Readable Travel Document
MRV	Machine Readable Visa (if followed by the letter A: refers to 80x120mm size; if followed by the letter B: refers to 74x105mm size)
MRZ	Machine Readable Zone
MS	European Union Member States
NFC	Near-Field Communication
NFIQ	Fingerprint Image Quality
NFP	National Facilitation Programme
NIR	Near-Infrared Range
NIST	National Institute of Standards and Technology
NUI	National Uniform Interface
OCR	Optical Character Recognition

OS	Operating System
PA	Passive Authentication
PAD	Presentation Attack Detection
PACE	Password Authenticated Connection Establishment
PAI	Presentation Attack Instrument
PC	Personal Computer
PDF	Portable Document Format
PKD	Public Key Directory
PNG	Portable Network Graphics
PNR	Passenger Name Record
ppi	Pixels Per Inch
PRADO	Public Register of Authentic travel and identity Documents Online
QR code	Quick Response code
RAU	Risk Analysis Unit
RFID-chip	Radio-Frequency Identification chip
RGB	Red, Green and Blue colour model
RIU	Research and Innovation Unit
RMT	Reduced Mobility Traveller
RP	Resident Permit
RPH	Resident Permit Holder
SBC	Schengen Borders Code
SCD	Standards and Capacity Development Sector
SIS	Schengen Information System (SIS II) (recast)
SLA	Service Level Agreement
SLTD	Interpol's Stolen and Lost Travel Document database
sBMS	Shared Biometric Matching Service
SOP	Standard Operating Procedure
SSS	Self-Service System
TA	Terminal Authentication
TCN	Third-Country National (non-European citizen)
TD	Travel Document (if followed by a number, it refers to a given size)
TEG	Technical Expert Group
TIFF	Tagged Image File Format (image file format)
UL 94	Standard for Safety of Flammability of Plastic Materials for Parts in Devices and Appliances testing
UMTS	Universal Mobile Telecommunications System
US/ USA	United States of America
UV	Ultraviolet electromagnetic radiation
VAU	Vulnerability Assessment Unit
VE	Visa Exempt
VH	Visa Holder
VIS	Visa Information System
VIZ	Visual Inspection Zone
WSQ	Wavelet Scalar Quantization (compression algorithm used for fingerprint images)

Terminology

The present terminology has been adopted in order to provide an unambiguous description of what SHOULD be observed in order to achieve a coherent approach with a common security baseline across Schengen borders.

SHALL This word, or the terms "REQUIRED" or "MUST", mean that the definition is an absolute requirement as stipulated in a regulation, its implementing acts and decisions.

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 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.

FRONTEX

EUROPEAN BORDER AND COAST GUARD AGENCY

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

PDF:
TT-03-20-651-EN-N
ISBN 978-92-9471-415-2
doi: 10.2819/814713

FPI: 20.0076

Publications Office
of the European Union