Technical Specifications for the Automatic Border Control Gates solution in “Narva 1” and Tallinn Airport Border Control Points

Annex 2

Contents:

FIGURES

TABLES

1 INTRODUCTION

Herewith the Contracting Authority has decided to initiate a project to introduce machine readable electronic travel document automated check for the following use cases of border crossers on the Schengen Border in Estonian Republic:

a) EU citizens subject to a 'minimum check' using travel documents;
b) Estonian and citizens of other EU countries according to the Contracting Authority list using national ID Card;
c) Citizens of third countries subject to the EES regulation, with whose country of residence Estonia has concluded an agreement under national facilitation program;
d) EU citizens if they use DTC Type 1 after the relevant EU regulation comes into force;
e) Citizens of third countries subject to the EES regulation using DTC Type 1, with whose country of residence Estonia has concluded an agreement under national facilitation program;
f) Citizens of third countries who have a valid Estonian residence permit;
g) Estonian citizens using DTC Type 2 credentials during the EU Commission pilot, expected in Q2 2027 – Q2 2028;

The aim of the project is to facilitate MRTD data self-service acquisition and delivery to the IT systems of the Estonian Police and Border Guard Board (PPGB) for quick processing of personal data and automate decision making process.

For accomplishing of the goals set the Contracting Authority intends to acquire a self-service ABC Gates solution providing more advanced and automated services for travelers than is in use at present ABC gates. The requirements in this Technical Specification are provided to explain the details of technical and procedural parameters to achieve the service level required. The ABC Gates Solution has to be designed in a way which allows the increasing the number and expanding the functionality of ABC gates in future developments. Foreseeable aspects of future upgrade and extension can be found in Chapter 16 of this Specification.

The Contracting Authority intends to tender the product as a 24/7/365 full time service. The ABC Gates Service provider will be responsible for maintaining the complete ABC gate system according to the Service Level Agreement key performance indicators, delivering the contents of the document and holder check to the PIKO (PBGB Border Control system) and operating the ABC gates according to the decisions delivered from PIKO. All the operations MUST be conformant to the requirements in this Technical Specification and relevant standards to guarantee trustworthiness and security of information sent for making border crossing decisions.

All the soft- and hardware needed for offering the ABC Gates service remains property of the ABC Gates Service provider. The Contracting Authority will install software needed for ABC Gates operators to both stationery and mobile workstations.

The ABC Gates Solution is classified as providing Self Service operations according to [BSI TR-03135-2] p.3.1.2 Application scenario - Self Service].
The ABC Gates solution is defined as a system that enables the realization of the use cases described above through the following operations:

EU citizens subject to a 'minimum check' using travel documents:

- Giving directions to the travelers crossing the border;
- Traveler eMRTD check;

- Facial biometric image capture according to the 1:1 document DG2 comparison profile and its quality requirements;
- Comparison of facial images from the facial image capture camera and eMRTD DG2;
- Delivery of the comparison result and content of DG1 to the PIKO system of the PBGB;
- Operating the gate doors and/or warning system depending on the decisions and commands from the PIKO system.
- Delivering information whether the border crossing event took place and alerts to PIKO;
- Interrupting automatic border crossing procedure and guiding travelers to the manual border control or 2nd level of inspection in case of errors in process.

Estonian and citizens of other EU countries according to the Contracting Authority list using national ID Card:

- Giving directions to the travelers crossing the border;
- Traveler ID Card check;
- Facial biometric image capture according to the 1:1 document DG2 comparison profile and its quality requirements;
- Comparison of facial images from the facial image capture camera and ID Card DG2;
- Delivery of the comparison result and content of DG1 to the PIKO system of the PBGB;
- Operating the gate doors and/or warning system depending on the decisions and commands from the PIKO system.
- Delivering information whether the border crossing event took place and alerts to PIKO;
- Interrupting automatic border crossing procedure and guiding travelers to the manual border control or 2nd level of inspection in case of errors in process.

Citizens of third countries subject to the EES regulation, with whose country of residence Estonia has concluded an agreement under national facilitation program:

- Giving directions to the travelers crossing the border;
- Traveler eMRTD check;
- National facilitation program membership and the existence of the EES file by PIKO;;
- Facial biometric image capture according to the 1:1 document DG2 comparison profile and its quality requirements;
- Comparison of facial images from the facial image capture camera and eMRTD DG2;
- Facial biometric image capture with second camera according to the EES face image quality requirements;
- Delivery of the 1:1 comparison result, EES compliant face image and content of DG1 to the PIKO system of the PBGB;
- Operating the gate doors and/or warning system depending on the decisions and commands from the PIKO system.
- Delivering information whether the border crossing event took place and alerts to PIKO;
- Interrupting automatic border crossing procedure and guiding travelers to the manual border control or 2nd level of inspection in case of errors in process.

EU citizens if they use DTC Type 1:

- Receiving DTC Type 1 with travel metadata to local temporary buffer;
- Traveler DTC Type 1 credentials pre-check (before arrival);
- Giving directions to the travelers crossing the border;
- Read the ICAO Barcode from the DTC app that refers to a previously sent DTC Type 1

- Traveler DTC Type 1 credentials check;
- Facial biometric image capture according to the 1:1 document DG2 comparison profile and its quality requirements;
- Comparison of facial images from the facial image capture camera and DTC Type 1 DG2;
- Delivery of the comparison result and content of DTC Type 1 DG1 to the PIKO system of the PBGB;
- Tapping NFC reader at second doors with closed passport for CA/AA verification;
- Operating the gate doors and/or warning system depending on the decisions and commands from the PIKO system.
- Delivering information whether the border crossing event took place and alerts to PIKO;
- Interrupting automatic border crossing procedure and guiding travelers to the manual border control or 2nd level of inspection in case of errors in process.

Citizens of third countries subject to the EES regulation using DTC Type 1:

- Receiving DTC Type 1 with travel metadata to local temporary buffer;
- Traveler DTC Type 1 credentials pre-check (before arrival);
- Giving directions to the travelers crossing the border;
- Read the ICAO Barcode from the DTC app that refers to a previously sent DTC Type 1
- Traveler DTC Type 1 credentials check;
- National facilitation program membership and the existence of the EES file by PIKO;
- Facial biometric image capture according to the 1:1 document DG2 comparison profile and its quality requirements;
- Comparison of facial images from the facial image capture camera and DTC Type 1 DG2;
- A facial image previously captured with the DTC Type 1 app or, in the absence of one, facial biometric image captured with second camera, according to the EES face image quality requirements;
- Delivery of the 1:1 comparison result, EES compliant face image and content of DG1 to the PIKO system of the PBGB;
- Tapping NFC reader at second doors with closed passport for CA/AA verification;
- Operating the gate doors and/or warning system depending on the decisions and commands from the PIKO system.
- Delivering information whether the border crossing event took place and alerts to PIKO;
- Interrupting automatic border crossing procedure and guiding travelers to the manual border control or 2nd level of inspection in case of errors in process.

Citizens of third countries who have a valid Estonian residence permit:

- Giving directions to the travelers crossing the border;
- Traveler eMRTD check;
- Facial biometric image capture according to the 1:1 document DG2 comparison profile and its quality requirements;
- Comparison of facial images from the facial image capture camera and eMRTD DG2;
- Delivery of the comparison result and content of DG1 to the PIKO system of the PBGB;
- Operating the gate doors and/or warning system depending on the decisions and commands from the PIKO system.
- Delivering information whether the border crossing event took place and alerts to PIKO;
- Interrupting automatic border crossing procedure and guiding travelers to the manual border control or 2nd level of inspection in case of errors in process.

Estonian citizens using DTC Type 2 credentials during the EU Commission pilot:

- Giving directions to the travelers crossing the border;
- Read the ICAO Barcode from the DTC Type 2 app that refers to DTC Type 2 credentials and communication protocol;
- Traveler DTC Type 2 check using RFID or Bluetooth BLE;
- Facial biometric image capture according to the 1:1 document DG2 comparison profile and its quality requirements;
- Comparison of facial images from the facial image capture camera and DTC Type 2 DG2;
- Delivery of the comparison result and content of DTC Type 2 DG1 to the PIKO system of the PBGB;
- Operating the gate doors and/or warning system depending on the decisions and commands from the PIKO system.
- Delivering information whether the border crossing event took place and alerts to PIKO;
- Interrupting automatic border crossing procedure and guiding travelers to the manual border control or 2nd level of inspection in case of errors in process.

It is recommended to treat the definitions and descriptions as described in “Machine Readable Travel Documents” [ICAO9303], FRONTEX “Best Practice Technical Guidelines for Automated Border Control (ABC) Systems” TT0415855ENN, “Best Practice Operational Guidelines for Automated Border Control (ABC) Systems” TT0415854ENN as well as in the ICAO “Technical Report on Machine Assisted Document Security Verification” ICAOMADSV1. Regarding modern electronic Identity Documents, the Technical Guidelines [BSI TR-03110], [BSI TR-03121], [BSI TR03127] and [BSI TR-03135] are recommended.

Unless otherwise stated, the requirements in this document apply to all software and hardware components offered by the ABC Gates Service provider in the framework of this Tender. All requirements SHALL be considered mandatory if not clearly specified otherwise.

All components supplied by the ABC Gates Service provider SHALL make it possible for the Inspection System and Inspection Application to completely implement and meet all relevant requirements of standards, regulations, guidelines and recommendations provided in Table 5 hereunder.

1.1 Scope Of Tender

Table 1 describes the scope of the components of the tender. Refer to Chapter 2 for further description of each component.

ABC Gates Solution component	Scope
Automatic Border Crossing service	The ABC Gates Service provider SHALL set up physically ABC gates, connected trough existing SMIT network to central ABC gates management and monitoring solution hosted in SMIT two data centers. We will call such a complete solution hereinafter ABC Gates solution. This solution MUST deliver to PBGB PIKO system information needed for making border crossing decisions using API and operating gates according to the API commands from the PBGB PIKO system. The ABC Gates Service provider SHALL integrate into ABC Gates solution the usage of Document PKI remote PA service from CA. The ABC Gates Service provider SHALL provide 24/7/365 maintenance and support by ABC Gates Service provider’s local representative office

	or local subcontractor according to the SLA requirements during the whole term of the Contract. The hard- and software upgrade schedule SHALL be agreed with the CONTRACT AUTHORITY, but the ABC Gates Service provider SHALL provide major upgrades to the ABC gates and mission and security critical updates upon their becoming available according to SLA requirements.
ABC Gates test solution	The ABC Gates Service provider SHALL set up physically one ABC gate at their premises in Estonia, connected to central ABC Gates management and monitoring test solution hosted in SMIT data center. Implementation of HA solution over two SMIT data centers is not required. Integration of ABC Gates test system with PIKO test system and Live Document PKI remote PA service is mandatory.
Tablets with protective covers and charging docks	6 portable devices for ABC Gates operators to use the ABC Gate management software.
ABC Gates operator software for tablets	Software used to operate automatic border control gates.
ABC Gates operator software for desktop workstations	Software used to operate automatic border control gates.
DTC Type 1 buffer	Software solution to receive DTC Type 1 with travel metadata from DTC Type 1 mobile apps or from eu-Lisa DTC Type 1 gateway and providing integration (APIs) with PIKO, ABC Gates solution and manual border control IS.
Licenses	All the licenses required to operate ABC Gates, contingent hard- and software.

Table 1: Scope of Tender

1.2 STRUCTURE OF THIS DOCUMENT

Chapter 2 contains overall requirements. Here descriptions of premises are provided, requirements to the gate modules and components etc. are described.

Chapter 3 contains requirements for system documentation. Documents mandatory to be provided by the ABC Gates Service provider are listed here.

Chapter 4 requirements to actual gate management. How to get access, how to manage data, how to react to commands and overrides are described here.

Chapter 5 contains technical requirements for the hardware. Physical and operational parameters and details of various hardware components of the ABC Gates solution are provided here.

Chapter 6 contains technical requirements to the management server capacity and monitoring server functionality.

Chapter 7 contains requirements to the procedures of document reading and verification process. Overall workflow, optical, electronic, biometric and combined checks are dealt with here.

Chapter 8 contains requirements and performance in handling defective documents.

Chapter 9 contains requirements for data exchange between user interfaces, PIKO and gates.

Chapter 10 contains monitoring and statistical data reporting.

Chapter 11 contains requirements for the security of the ABC Gates solution.

Chapter 12 contains service compliance requirements.

Chapter 13 contains requirements for the service level agreement.

Chapter 14 contains statics and reporting requirements.

Chapter 15 contains additional information.

Chapter 16 contains training requirements.

Chapter 17 contains requirements definition and tender evaluation example

1.3 TERMINOLOGY

Requirements as defined in this Specification can be mandatory, recommended or optional. All the requirements in this document are mandatory if not otherwise clearly specified.

MUST, SHALL, REQUIRED, NORMATIVE	The implementation is an absolute requirement of the specification and must be used/included.
RECOMMENDED, NOT RECOMMENDED, SHOULD, SHOULD NOT	The requirements are recommendations, this means that there may be valid reasons in particular circumstances to ignore a particular item or requirement, but the full implications must be understood and carefully weighed before choosing a different course.
MAY, OPTIONAL	The requirements are not binding. ABC Gates Service provider may choose to include it; another may omit it.
MUST NOT, SHALL NOT	A so-called requirement is an absolute prohibition of the specification.

Table 2: Interpretation of keywords

1.4 DEFINITIONS AND ABBREVIATIONS

1.4.1 DEFINITIONS

Term	Definition
Contracting Authority	The term Contracting Authority is used to refer to (SMIT) as responsible for the tender process and as responsible Commissioning Party.
DTC	Digital Travel Credentials – the digital version of the data stored on travel document chip datagroups DG1, DG2.
EAC-PKI	Extended Access Control Public Key Infrastructure – the infrastructure required to control read access to fingerprint biometrics on Passports and Travel Documents through Extended Access Control.
EES	The Entry/Exit System (EES) is an automated IT system for registering non-EU nationals travelling for a short stay, each time they cross the external borders.
eMRTD	Term used to encompass all electronic Machine Readable Travel Documents, hereunder electronic Passports, Residence Permits, Local Border Traffic Permits and National Identity Cards containing ICAO Doc 9303 compatible RFID chip and acceptable by law for Schengen Border crossing.
Gate module	Self-standing set of 1 (one), 2 (two), 3 (three) or 4 (four) individual gates.
Inspection Application	Software supervising document reading, face enrollment, biometric comparison, data delivery to the PIKO interface and guiding the gate doors.
Inspection System	In the scope of the present tender the system contains document reading hard- and software, facial image comparison software and user interface to display information to the person passing a gate. Inspection System gets its input data from a full-page flatbed document reader and facial image capture camera. Hard- and software for fingerprint enrollment and comparison will be added when corresponding upgrade to the system will be made.
Internal Defect List	The defect list is used for internal purposes, in particular for border control. It MUST contain all known defects.
Terminal	Inspection System (IS) as defined in [BSI TR-03110-1] p.2.2.
Travel Document	An identity document compliant to [ICAO9303] and acknowledged as such due to [ICAO9303] or international agreements.

Operator	Terms are used to cover all human personnel that require system access to operate, administer or audit the ABC gates.
PBGB	Police and Border Guard Board
PIKO	Border Control System of the PBGB.
ABC Gates Service provider	The term is used throughout this specification to refer to the vendor, tenderer/bidder or contractor in all phases of the procurement and delivery of the requested ABC Gates solution.

Table 3: Definitions

1.4.2 ABBREVIATIONS

AA	Active Authentication
AB	Absorbent
ABC	Automated Border Control
BAC	Basic Access Control
BCP	Border Control Point
CA	Chip Authentication
CAN	Card Access Number
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
CS-PKI	Country Signing Public Key Infrastructure
CVCA	Country Verifying Certification Authority
DET	Detection Error Trade-Off
DGn	LDS data group n
DH	Diffie-Hellmann
DL	Defect List
DSL	Document Signer List
DTC	Digital Travel Credentials
DTC-VC	Digital Travel Credentials Virtual Component
DTC-PC	Digital Travel Credentials Physical Component

EAC	Extended Access Control
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellmann
EF.COM	Header and Data Group Presence Information
$EF.SO_D$	LDS Security Object
e-ID	Electronic identity document
eMRTD	Electronic Machine Readable Travel Document
ePass	Electronic Passport
eRP	Electronic Residence Permit
FAR	False Acceptance Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Rejection Rate
GDPR	The EU General Data Protection Regulation
HA	High Availability
ICAO	International Civil Aviation Organisation
IR	B900 spectral range infrared
IS	Inspection System, Information System
LDS	Logical Data Structure according to ICAO Doc 9303
ML	Master List
MR	MRZ area
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
NIST	National Institute of Standards and Technology (US)
NTWG	ICAO New Technology Working Group
OK/NOK	Positive or negative result of a check
PA	Passive Authentication

PAD	Presentation Attack Detection
PBGB	Estonian Police and Border Guard Board
PKI	Public Key Infrastructure
RSA	Rivest Shamir Adleman
SMIT	IT and Development Centre, Ministry of the Interior
SO_D	Document Security Object
TA	Terminal Authentication
TCC	Terminal Control Centre
TLS	Transport Layer Security
UI	User Interface
UPS	Uninterruptible Power Supply
UV	365 nm range wavelength ultraviolet light
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
VI	Visual (white) light

Table 4: Abbreviations

1.5 REFERENCES AND STANDARDS

#	Standard	Publisher	Date
[BSI TR-03105-5.1]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03105 Part 5.1, version 1.5: Test plan for ICAO compliant Inspection Systems with EACv1.	BSI	February 10th, 2020
[BS TR-03105-5.2]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03105 version 1.2, Conformity Tests for Official Electronic ID Documents, Part 5.2, version 1.2 Test plan for eID and eSign compliant eCard reader systems with EAC 2	BSI	November 19th, 2019

[BSI TR 03105-4]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03105 version 3, Part 4. Test Plan for ICAO-compliant Proximity Coupling Devices (PCD) on Layers 1-4		November 11th, 2016
[BSI TR-03110-1]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03110-1 version 2.10, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 - eMRTDs with BAC/PACEv2 and EACv1.	BSI	March 20th, 2012
[BSI TR-03110-3]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03110-3 version 2.10, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specifications	BSI	March 20th, 2012
[BSI TR-03121]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline Biometrics for Public Sector Applications, v.7	BSI	November 1st, 2025
[BSI TR-03135]	Bundesamt für Sicherheit in der Informationstechnik, Machine Authentication of MRTDs for Public Sector Applications Version 5.0.0	BSI	October 28th 2025
[BSI TR-03135-1]	Bundesamt für Sicherheit in der Informationstechnik, Machine Authentication of MRTDs for Public Sector Applications, Part 1, Version 5.0.0	BSI	October 28th 2025
[BSI TR-03135-2]	Bundesamt für Sicherheit in der Informationstechnik, Machine Authentication of MRTDs for Public Sector Applications, Part 2, Version 5.0.0	BSI	October 28th 2025
[EN 62368-1]	Audio/video, information and communication technology equipment - Part 1: Safety requirements.	EN	2024
[EN62471]	Photobiological safety of lamps and lamp systems.		2008

[ISO/IEC 27001:2022]	Information security, cybersecurity and privacy protection — Information security management systems — Requirements.		2022
[ISO/IEC 19794-5:2011]	v Information technology — Biometric data interchange formatsPart 5: Face image data		2024
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 (EES)		2019

Table 5: References

2 GENERAL DESCRIPTIONS

2.1 NEW GENERATION OF ABC GATES

Due to the need to expand the functionality of ABC gate while ensuring uninterrupted service operation, it is necessary to change the approach to the management of ABC gate hardware and software changes. Considering that changes to the ABC gate design are the most complex and time-consuming, both a modular approach and the immediate implementation of the hardware necessary to implement all the foreseen functionalities should be initially envisaged. For the successful implementation of subsequent software changes, it is necessary to ensure the immediate integration of all necessary hardware components (except the fingerprint reader) into the ABC Gates solution. In the case of the fingerprint reader, a modular approach must be provided, which would later allow us to use either contact or contactless devices.

The ABC Gates solution must assume that meeting the quality requirements for EES biometrics capture must not reduce the throughput of the ABC gate in other scenarios.

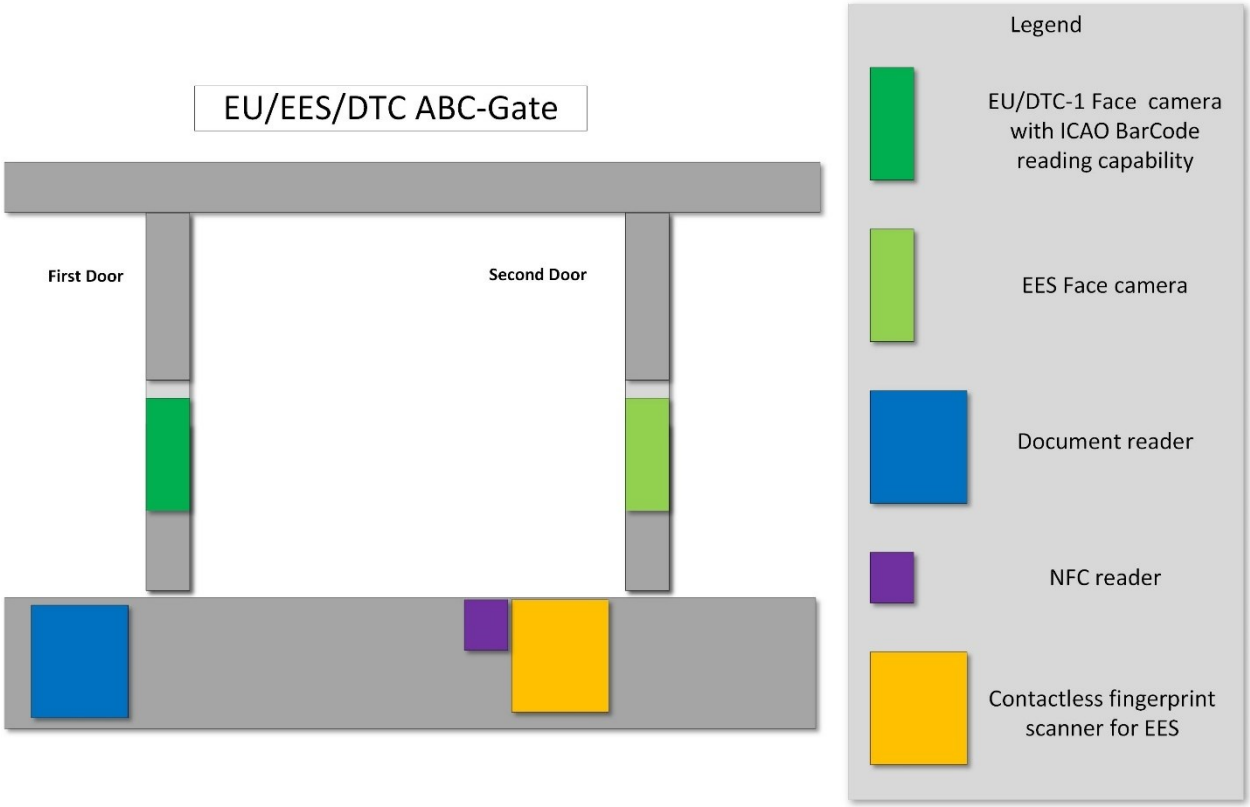

Figure 1. Conceptual ABC Gates solution

2.2 BACKGROUND INFORMATION

ABC Gates will be installed initially in two locations – Lennart Meri Tallinn Airport BCP and 'Narva 1' BCP for both entry and exit.

2.1.1 LENNART MERI TALLINN AIRPORT BCP

Considering the Tallinn Airport expansion project, 4+4 abc gates will be installed initially. 4 of them are planned for the entry direction in a temporary area and will later be relocated together with the increase in the number of gates to 9. 4 exit direction gates will initially be installed in place of the old, dismantled ABC gates, also in a temporary area. Upon completion of the repair work on the departure direction, the ABC gates will be relocated, and the number will be increased to 8.

On the following Figures the plans of the premises in the Tallinn Airport will provide an overview of the location of the ABC gates:

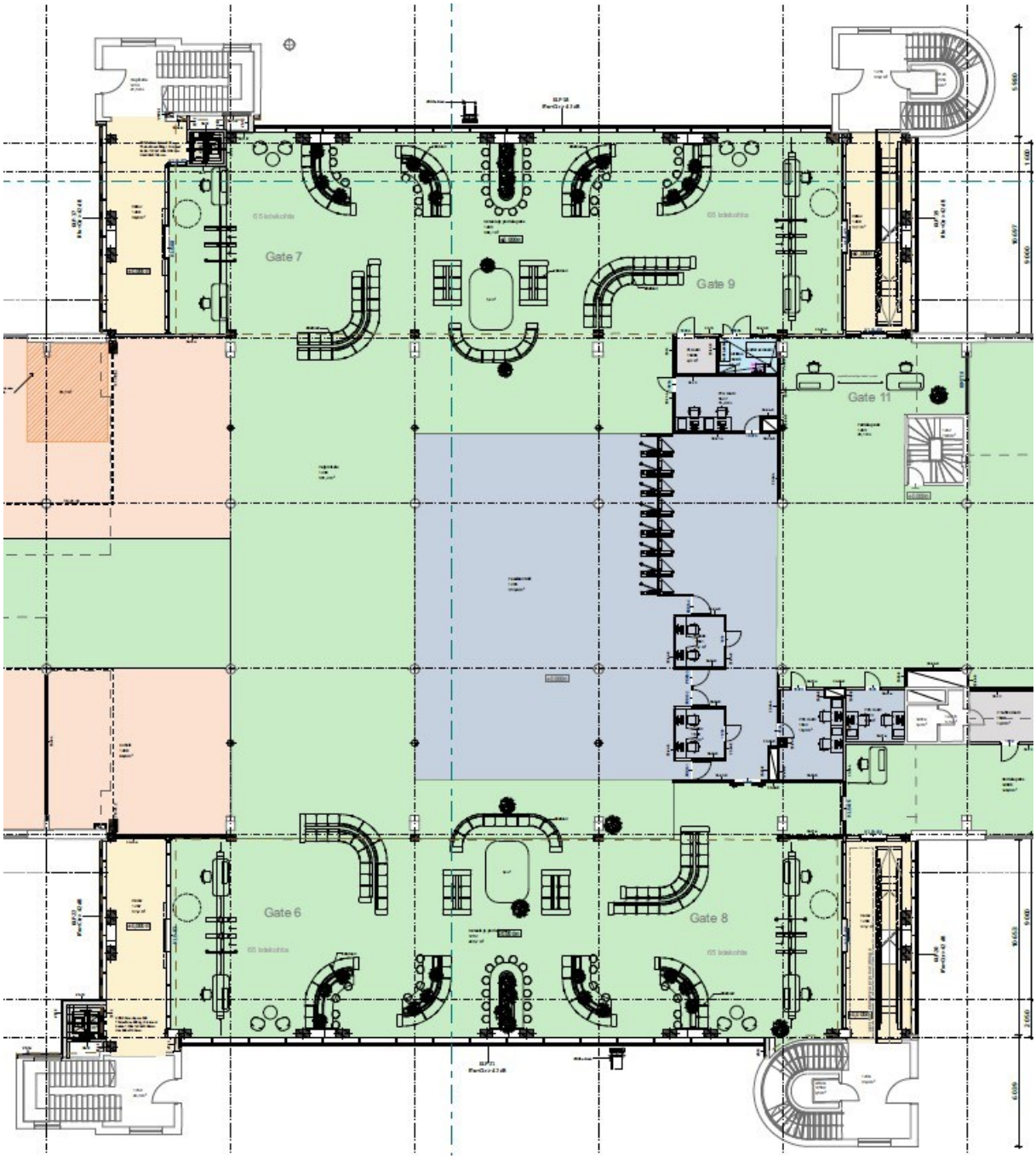

Figure 2. Final ABC gates module location in Lennart Meri Tallinn Airport BCP exit

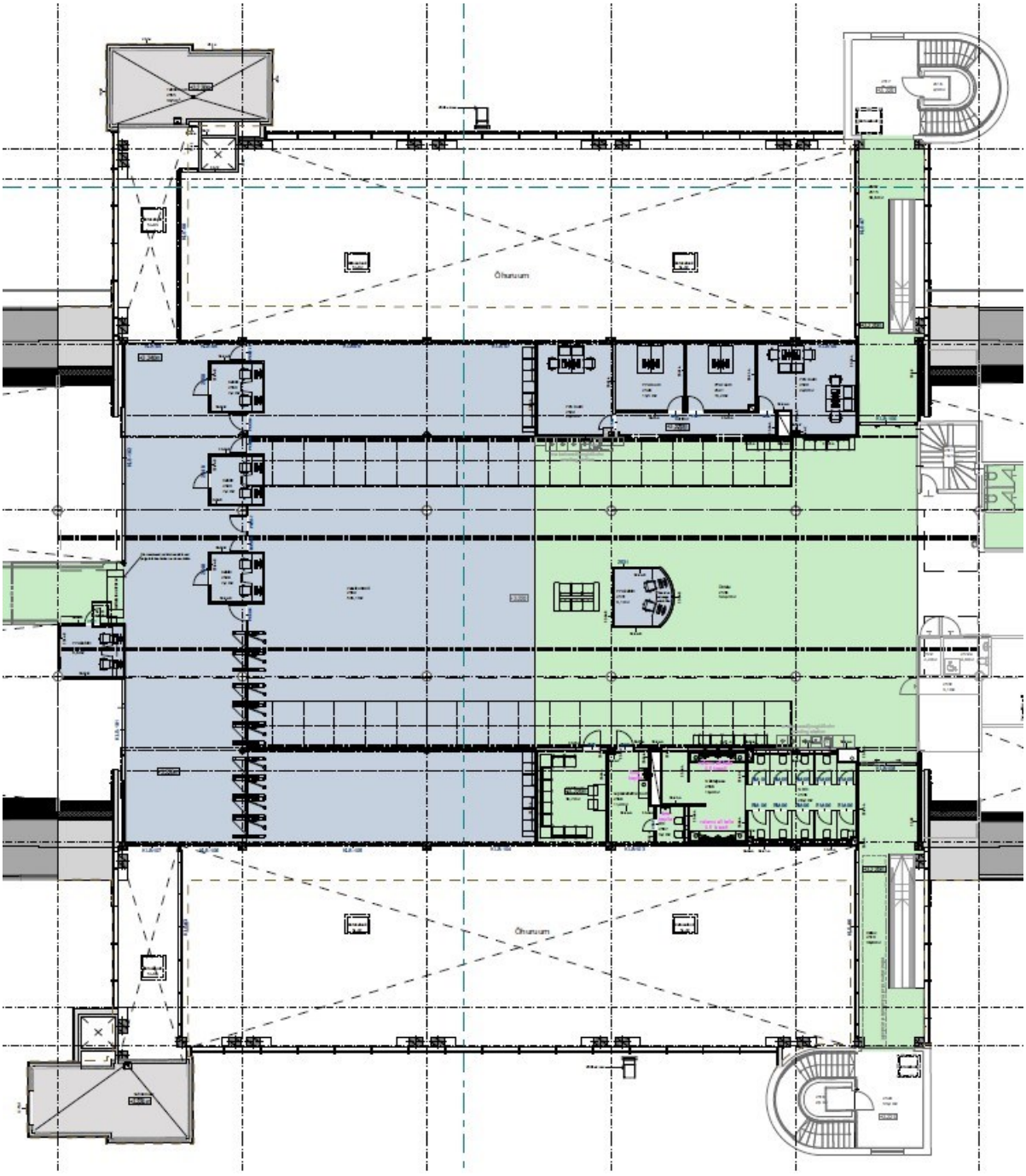

Figure 3. Final ABC gates module location in Lennart Meri Tallinn Airport BCP entry

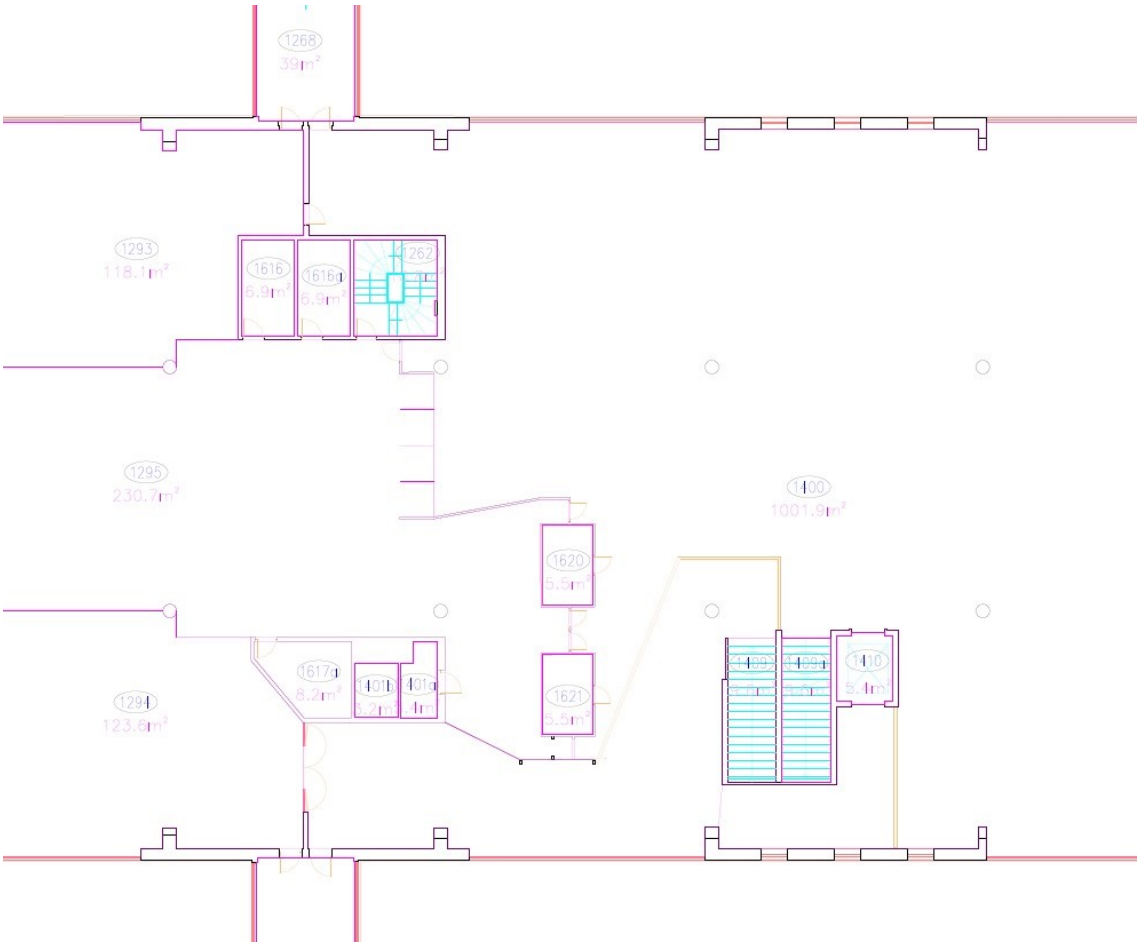

Figure 4. Temporary ABC gates module location in Lennart Meri Tallinn Airport BCP exit

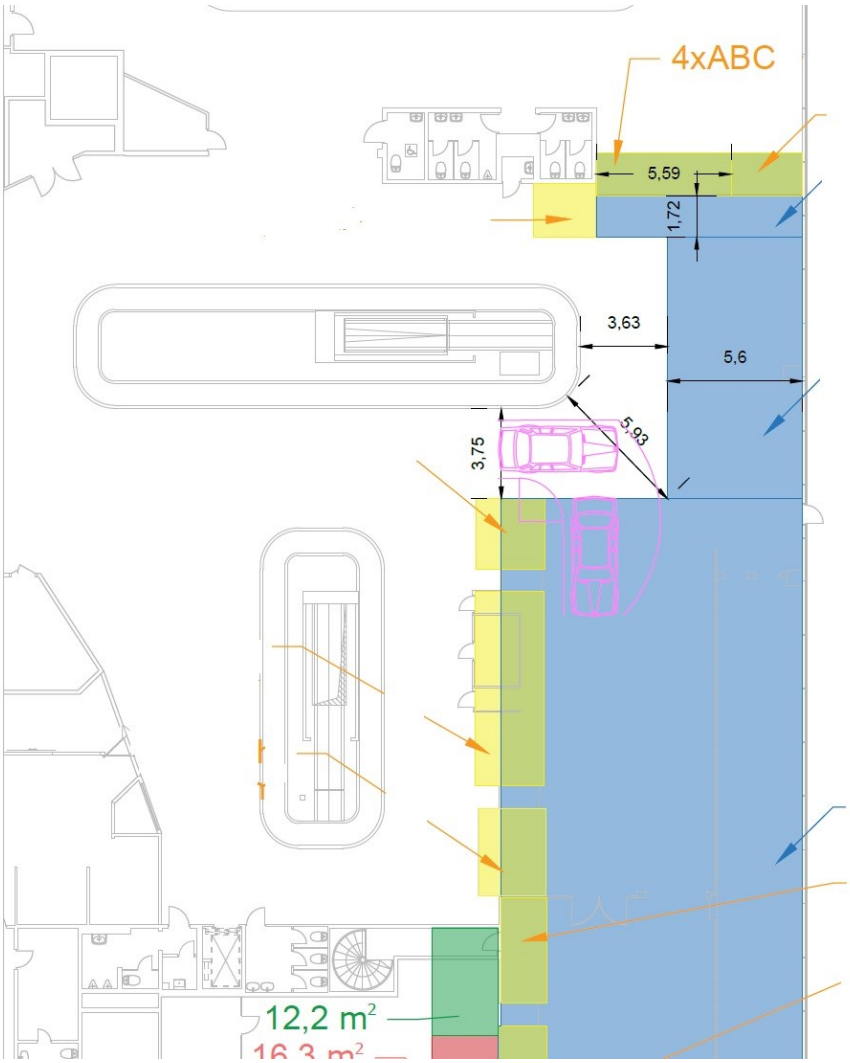

Figure 5. Temporary ABC gates module location in Lennart Meri Tallinn Airport BCP entry

2.1.2 'NARVA 1' BCP

Narva 1 BCP 3 exit and 4 entry ABC gates will be installed.

On the following Figure the plan of the premises in the Narva 1 BSP will provide an overview of the location of the gates:

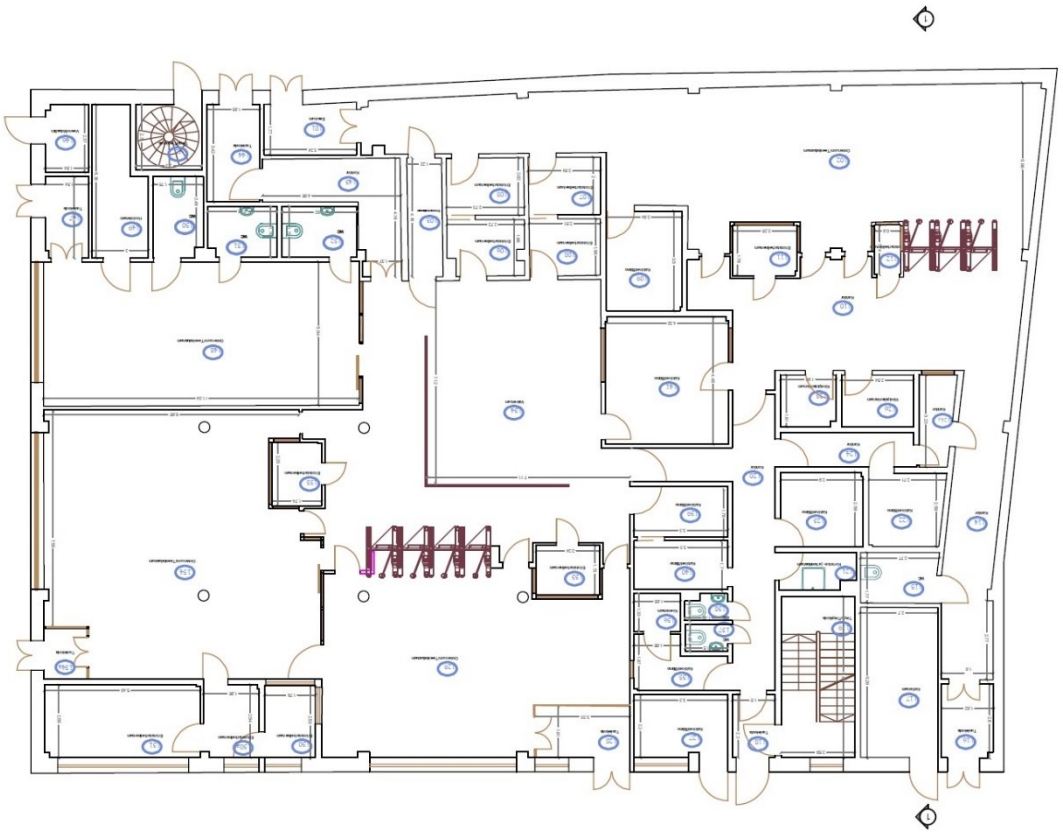

Figure 6. ABC gates modules location in ‘Narva 1’ BCP exit and entry

2.1.3 POWER SUPPLY

1-phase 230V 50Hz AC power will be available at Lennart Meri Tallinn Airport and ‘Narva 1’ BCP.

2.2 SAFETY

All equipment and fittings MUST comply with EU safety requirements and applicable standards.

2.3 ABC GATES IMPLEMENTATION STAGES AND DEADLINES

The following circumstances have been considered when defining the stages of ABC Gates implementation and preparing the schedule:

a. Tallinn Airport expansion works will start in June-July 2026 and will last until the end of 2027.

b. The existing ABC Gates agreement is valid until 31.12.2026

c. In Q2-Q3 2027, it is intended to launch additional functionalities related to the EU Commission DTC Type 2 pilot project in ABC Gates

d. During 2027, a national facilitation program for third-country nationals will be implemented within the framework of the EES.

e. In 2028, DTC Type 1 functionality will be implemented after the relevant EU regulation enters into force.

STAGE NR.	STAGE DESCRIPTION	DEADLINE	NOTES
1	Tallinn Airport BCP Entry. 4 ABC gates in temporary entry area.	Nine months after signing the contract.	Critical deadline.
2	Tallinn Airport BCP Exit. 4 ABC gates in existing exit area.	Nine months after signing the contract.	Critical deadline.
3	Narva 1 BCP Entry. 4 ABC gates.	Nine months after signing the contract.	
4	Software Upgrade for Tallinn Airport BCP ABC gates to support DTC Type 2 pilot	Two months after implementing ABC Gates in Tallinn Airport.	Preliminary deadline.
5	Implementation of EES workflow and functionality in all ABC gates.	Three months after implementing ABC Gates in Tallinn Airport.	Preliminary deadline.
6	DTC Type 1 capability implemented in all ABC gates.	Eighteen months after implementing ABC Gates in Tallinn Airport.	Preliminary deadline, may change due to the unknown implementation deadline set in the EU laws under preparation,
7	Relocation to final location 4 existing ABC gates Tallinn Airport BCP Entry and installation of 5 additional ABC gates there.	Twelve months after implementing ABC Gates in Tallinn Airport.	Preliminary deadline, depends on the completion of the expansion works of Tallinn Airport.
8	Relocation to final location of 4 existing ABC gates Tallinn Airport BCP Exit and installation of 4 additional ABC gates there.	Twelve months after implementing ABC Gates in Tallinn Airport.	Preliminary deadline, depends on the completion of the expansion work of Tallinn Airport.
9	Narva 1 BCP Exit. 3 ABC gates.		

Table 6: Implementation stages

2.4 MAJOR OVERVIEW OF THE ABC GATES SOLUTION

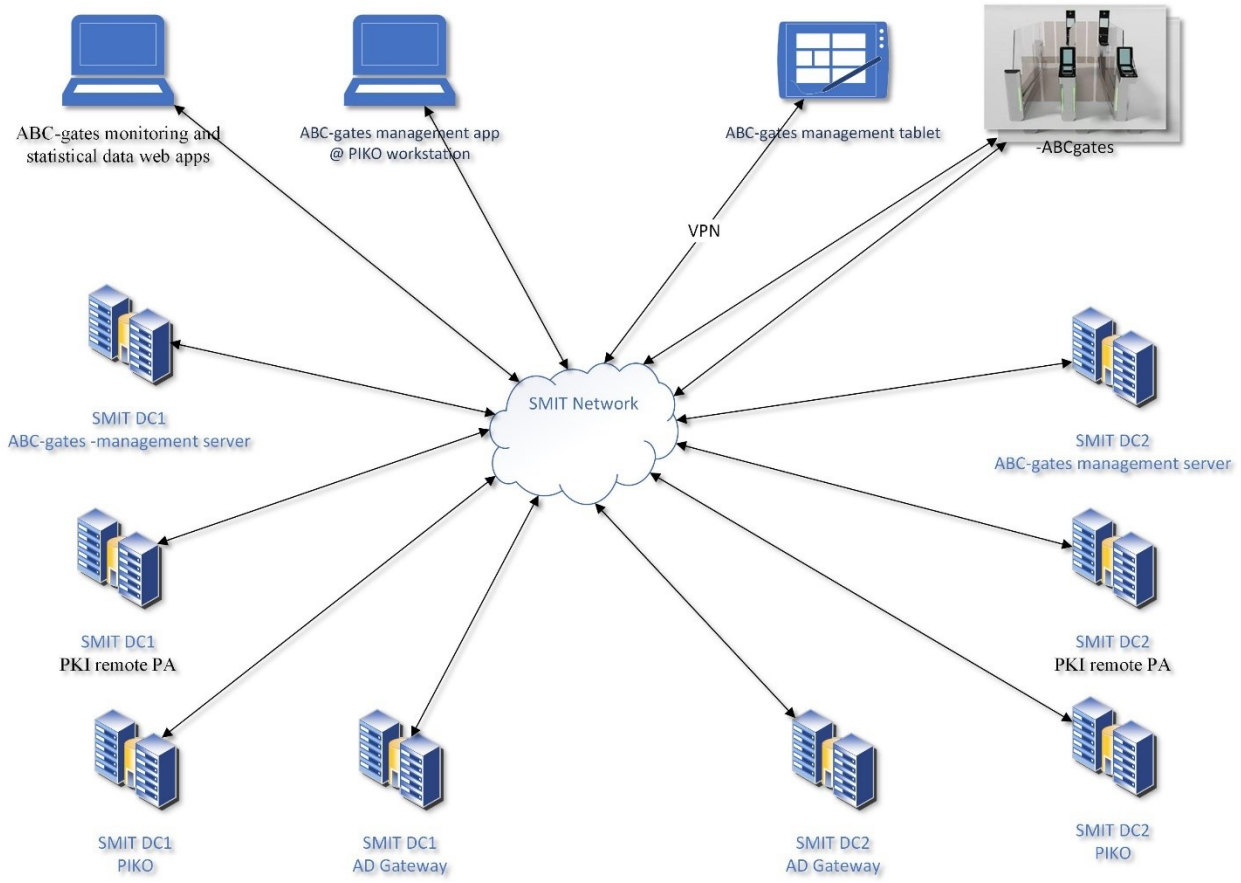

Figure 8. Schematic description of the ABC Gates solution

Figure 8 provides a schematic overview of the requested ABC Gates solution. The figure serves the purpose of functional specification and scoping only. The CONTRACT AUTHORITY accepts that the naming of systems or components of the ABC Gates Service provider offered solution may differ from the naming used in this document. The Contracting Authority also accepts that the ABC Gates Service provider's solution might be implemented in a way that systems or system components are combined or linked in a different manner than reflected in Figure 8.

The ABC Gates will be connected to Border Control (PIKO) system via two interfaces through management servers by two independent HA Data Centers used by ABC Service Provider and running the Management and Monitoring software.

More detailed requirements for functional components in Figure 8 are provided in the following sub-chapters.

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 1.	The ABC Gates Service provider SHALL submit proof that he has all the licenses required to operate ABC Gates, contingent hard- and software. Licenses MUST cover all the components purchased in course of this Tender.		

2.5 ABC GATES MODULE CONFIGURATION

All drawings containing the ABC gates modules have only informative purposes about positioning and are not meant to be neither recommendations nor requirements of detailed design. The ABC Gates Service providers are free to propose ABC gates module designs as they consider appropriate and in compliance to TT0216152ENN, TT0415855ENN and TT3012750ENN.

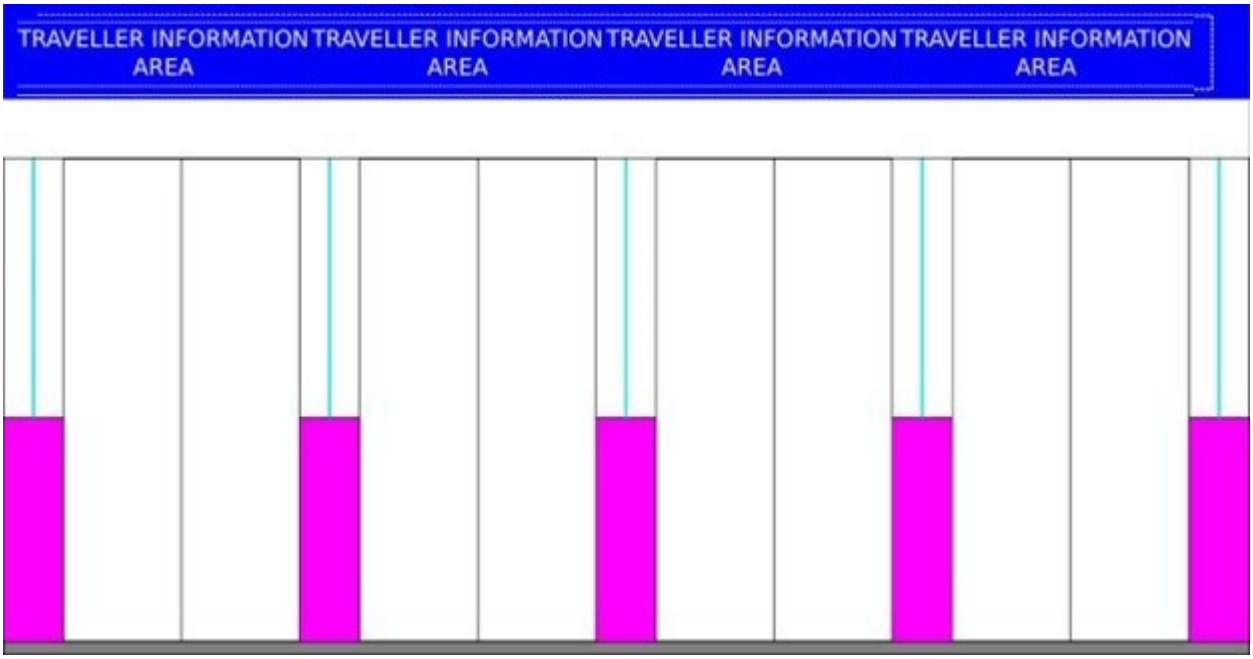

Figure 9. Schematic frontal view of the primary version of the ABC gates module.

Figure 9 provides concept of the physical design of primary ABC gates module consisting of a set of ABC gates and separate light boxes. The number of ABC gates depends on the location.

2.5.1 REQUIREMENTS TO GATE MODULE CONSTRUCTION

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 2.	To be future-proof, an ABC Gates solution MUST be designed and configured so that it does not preclude any future enhancements for document authentication modules or biometric systems for the lifetime of the hardware – a modular standard solution. ABC Gates MUST have designated locations allowing quick installation and implementation of fingerprint readers when EES functionality is implemented.		

REQ 3.	Footprint images MUST be drawn on the floor indicating the standoff distance in front of the camera for both cameras located in front/inside of both first and second doors.		
REQ 4.	Cameras MUST support range of subject heights at standard standoff distance between 1.4 and 2.1 meters.		
REQ 5.	A ABC Gates module MUST contain at least: • 1, 2, 3 or 4 individual gates; • A set of restrictive glass doors; • Facial image capture cameras; • Document readers; • Physically separate display boxes carrying information for the travelers to be installed above the gate and having width equal to the concrete gate.		
REQ 6.	The placement of the display boxes will be determined by the ABC Gates Service provider. Detailed contents, colors, placement and means of installation will be specified and agreed with the PBGB during execution of the Contract.		
REQ 7.	Display boxes management solution MUST be enable for ABC Gates operator change visual tags in display box of each gate describing the passenger categories (EU, other countries ISO 3166-1 alpha-2 codes) or functionality (Passport, ID Card, DTC etc) in real time along with enabling/disabling the gate functionality that supports it from gate operator management software.		
REQ 8.	To be future-proof, gate modules must be easily horizontally expandable by means of installing individual gates together with double-layer floor to the existing gate modules.		
REQ 9.	The gates ergonomics, dimensions, location and the environmental conditions SHOULD be considered with a special focus on the needs of travelers with disabilities. NOTE: Handicapped people in wheelchairs or similar will be directed to operator-assisted border crossing control.		
REQ 10.	The design of the gates SHOULD be planned with consideration for the usage of trolleys and other luggage (e.g. duty-free bags).		

REQ 11A.	Design of gate modules SHOULD make the best use of available space in a way that caters to all users. Gate module measurements MUST not exceed following measurements: • 4-gate configuration – 5280 (W) * 2400 (H) * 3200 (D) millimeters; • 3-gate configuration – 4024 (W) * 2400 (H) * 3200 (D) millimeters; • 2-gate configuration – 2768 (W) * 2400 (H) * 3200 (D) millimeters; • 1-gate configuration – 1512 (W) * 2400 (H) * 3200 (D) millimeters.		
REQ 11B.	Following gate module internal dimensions for interlocking area MUST be guaranteed: • Minimal width – 900 millimeters: • Minimal length – 1200 millimeters.		
REQ 12.	A gate module MUST have rigid self-standing construction that can be fastened to the floor by means of gluing. The rooms in Narva 1 BCP have floor heating installed, and this MUST be considered in choice of gate materials and adhesive.		
REQ 13.	All fastenings MUST be covered, or special tools MUST be used to operate.		
REQ 14.	There MUST be glass walls present between individual gates. Overall design of gate modules in form of technical drawings and photo of the physical gate or gate module SHALL be provided by the ABC Gates Service provider and agreed with the PBGB during execution of the Contract.		
REQ 15.	A gate module MUST have double-layer floor without distinctive edges to prevent stumbling. The thickness of the floor MUST NOT exceed 5 centimeters.		
REQ 16.	The floor MUST contain supportive beams increasing rigidity of the gate module.		
REQ 17.	A gate module MUST meet basic requirements regarding the physical installation and security and safety considerations. This includes protecting the modules which are installed in public areas against tampering and vandalism: • by using materials that are scratch proof; • by using materials that are impact-resistant; and preferably stainless steel and tempered glass.		
REQ 18.	The physical parts of the gate modules MUST comply with the applicable fire protection requirements.		

REQ 19.	The gate units MUST contain lighting modules to ensure proper illumination of the traveler's face in front of both cameras.		
REQ 20.	The display boxes above the ABC gate modules MUST provide automatically adjustable brightness depending on the room illumination level between 200-2000 nits.		
REQ 21.	Graphics with multiple colors or harsh contrasts SHOULD be avoided.		
REQ 22.	Access route openings (door frames) in Tallinn Airport and 'Narva 1' BCP have minimum measurements 1000*2100 millimeters. This MUST be taken into consideration while developing mechanical design and installation of the gate modules.		
REQ 23.	Independent switching off every individual gate MUST be supported.		
REQ 24.	Every individual gate MUST have internal independent main circuit breaker.		
REQ 25.	Every individual gate MUST have internal independent UPS which ensures the gate operation for 30 minutes.		

2.5.2 DOORS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 26.	Gate module normally closed doors MUST restrain trespassing of travelers through the gate in working state. Actual design of the doors restricting trespassing MUST be compliant to FRONTEX Best Practice Guidelines TT0216152ENN, TT0415855ENN and TT3012750ENN .		
REQ 27.	Door leaves MUST be clamped down when in closed position to prevent opening them by mechanical force.		
REQ 28.	In case a ABC gate is out of service, there MUST be an option to physically close this ABC gate in order to prevent travelers from inadvertently trying to use it.		
REQ 29.	Some mechanical / accompanying noise is RECOMMENDED allowing the traveler to realize that the ABC gate has opened taking account travelers with disabilities.		

REQ 30.	It MUST be ensured that the ABC gate doors do not close on travelers, especially if they move slowly or if they have difficulties with orientation due to a disability or age.		
REQ 31.	Movement of the door leaves MUST be stopped if the movement is restricted to prevent damage to the passengers or any other objects.		
REQ 32.	An alert about movement restriction SHALL be sent to the ABC Gates operator workstation UI and logged in the system.		
REQ 33.	Door leaves MUST be made of impact resistant security glass.		
REQ 34.	Door leaves MUST be covered with clear transparent security foil.		

2.5.3 DOCUMENT READER

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 35.	e-Passport readers SHOULD be at average elbow height and placed on the right-hand side of the gate.		
REQ 36.	MRTD MUST be placed on the document reader with the biographical data page facing down and the MRZ side first according to Figure 10.		
REQ 37.	Document reader MUST be able to communicate with RFID chips in both locations – either in MRTD data page or back cover.		
REQ 38.	Document readers MUST be full-page type. Swipe-type document readers MUST NOT be used.		
REQ 39.	Document Reader MUST be supplied together with document model catalogue in machine readable form according to the defined XML schema of [BSI TR-03135] which summarizes all necessary information on the spectrally selective verification checks.		
REQ 40.	Automated reading, decoding and verification of following 2D barcodes MUST be supported: ICAO Digital Barcode (from mobile phone screen) EU Schengen Visa sticker 2D barcode (passport)		
REQ 41.	Document readers MUST be able to communicate with NFC and Bluetooth 6.0, including Bluetooth Low Energy (BLE) for DTC Type 1 and Type 2 implementations.		

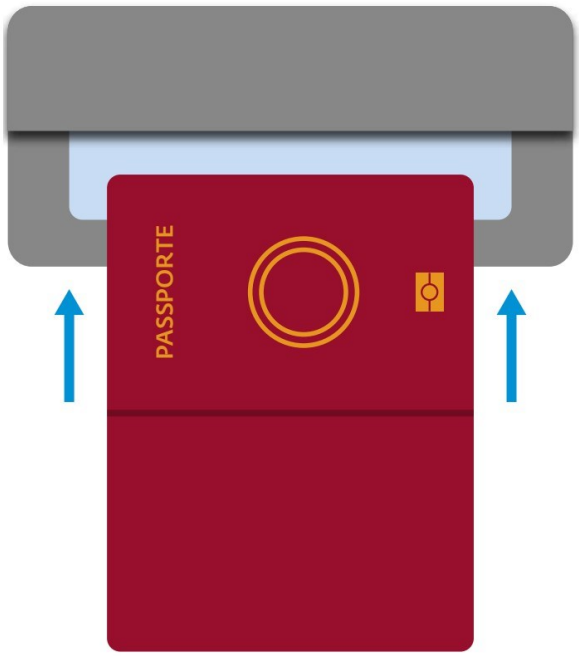

Figure 10: Graphic instruction on how to place the e-Passport on the reader

2.5.4 FACIAL IMAGE CAPTURE CAMERA

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 42.	There MUST be two facial image capture cameras per one gate.		
REQ 43.	The default height setting of the self-adjusting camera MUST configurable.		
REQ 44.	Facial image capture camera MUST have optical autofocus.		
REQ 45.	Facial image capture camera which is located at the first door MUST be able to capture face image under 2s for 1:1 matching with travel document chip DG2.		
REQ 46.	Facial image capture camera which is located at the second door MUST be able to capture face image under 8s and meet all the EES facial enrollment quality requirements.		

2.5.5 USER INTERFACES (SCREENS)

2.5.5.1 TRAVELLERS' SCREENS INTERFACE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 47.	Screens MUST be large enough to be observed by the travelers queuing to use the gates.		

REQ 48.	The screens must offer guidance and live video feedback to the traveler (digital mirror).		
REQ 49.	Screen position MUST be selected based on ergonomics and convenience to the travelers.		
REQ 50.	Screens MUST be located at or inside of both (first and second) gate doors.		

2.5.5.2 GATE OPERATOR'S DESKTOP WORKSTATION INTERFACE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 51.	Gate management UI (Gate monitoring area) MUST show at the same time: • Status of up to ten gates; and Alerts from the PIKO system.		
REQ 52.	Details of the gate operator's desktop workstation user interface SHALL be agreed with the Contracting Authority during the execution of the Contract.		

2.5.5.3 GATE OPERATOR MOBILE INTERFACE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 53.	Gate management UI (Gate monitoring area) MUST show at the same time: • Status of up to ten gates; and • Alerts from the PIKO system.		
REQ 54.	Details of the gate operator's mobile user interface SHALL be agreed with the Contracting Authority during execution of the Contract.		

2.5.6 PLACEMENT OF THE EQUIPMENT/HARDWARE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 55.	All hardware except the facial image capture cameras, document readers and fingerprint readers needed for operating the ABC gates MUST be in the closed wall spaces of gate modules.		

REQ 56.	The ABC Gates Service provider MUST install UPS-s and other supporting hardware in the closed wall spaces of ABC gate modules.		

2.5.7 GATE IDENTIFICATION

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 57.	Each ABC Gates installation, as well as each of ABC gate modules and individual gates SHOULD be uniquely identified.		

2.5.8 NETWORK CABLING AND CONNECTIONS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 58.	Cabling between gate modules at the same BCP MUST be installed in conduits preventing intentional and unintentional damage and intrusion.		
REQ 59.	All network and power supply cabling MUST be positioned overhead or within the double floor. Outside from the gate module cabling MUST be positioned only overhead.		

2.5.9 GATE OPERATING CONDITIONS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 60.	The Gates MUST be operative at ambient temperatures 5 – 40 degrees Centigrade.		
REQ 61.	The Gates MUST be operative at ambient humidity 30 – 70 per cent.		
REQ 62.	Individual gate availability requirements will be provided in the SLA, Chapter 14.		

2.6 REQUIREMENTS TO GATE FUNCTIONALITY

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 63.	The gate MUST have functionality to detect passing the gate and direction of movement of the traveler.		
REQ 64.	The gate MUST have functionality to sense/register tailgating. In case of tailgating information about this event MUST be logged and forwarded to the ABC Gates operators.		
REQ 65.	The gate MUST have IS client functionality for CSCA (and CVCA) PKI operations.		

3 REQUIREMENTS TO SYSTEM DOCUMENTATION

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 66.	The ABC Gates Service provider SHALL provide general system documentation written in Estonian covering the following items: • ABC Gates operator desktop workstation and mobile UI operating manuals.		

4 REQUIREMENTS TO THE ABC GATEs MANAGEMENT SOLUTION

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 67.	The ABC Gates management solution MUST have GUI for desktop computers.		
REQ 68.	The ABC Gates management solution MUST have GUI for tablets.		
REQ 69.	Personal data acquired during passenger check MUST NOT be stored in the management and monitoring system except when failed border crossings occurred or MAD is given positive results. Records of these events must be kept for 14 days.		

REQ 70.	ABC Gates Service provider MUST provide the secure access to the abc-gates monitoring and statistical data by providing access to monitoring and statistics system(s) to representative(s) of PBGB. Detailed configuration of the rights/roles will be agreed during the course of the Contract but before launching the service.		
REQ 71.	Management servers operating mode MUST be active/active (HA).		
REQ 72.	Monitoring servers operating mode MUST be active/passive.		
REQ 73.	Manual override by the ABC Gates operator of the status (operational/non-operational) of an individual gate MUST be supported.		
REQ 74.	Manual override by the ABC Gates operator of the operating commands delivered from PIKO MUST be supported.		
REQ 75.	Operating of the ABC gates MUST be based only on the decisions and commands from PIKO or as manual override. No decision to open the doors SHALL be made in the gate management system.		

5 TECHNICAL REQUIREMENTS TO THE HARDWARE

5.1 DOCUMENT READER

5.1.1 DOCUMENT FORMATS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 76.	Document reader MUST support TD1 format of MRTDs specified in [ICAO9303]		
REQ 77.	Document reader MUST support TD3 format of MRTDs specified in [ICAO9303]		

5.1.2 READING THE OPTICAL DATA

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 78.	Document data page SHALL be optically recorded and digitized under IR, VI and UV spectral range light.		

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 79.	The optical resolution SHALL be at least 385 ppi.		
REQ 80.	Reading of MRZ and CAN MUST be supported.		
REQ 81.	Document reader sensitivity to incoming ambient light MUST be minimized by: • shielding by technical safeguarding measures; • by compensating of external light; or by both methods.		
REQ 82.	OCR of data both in MRZ and CAN MUST be supported.		
REQ 83.	OCR of data for tests MUST be based on the IR B900 spectral range image. In case of failure of reading in IR spectral range the system SHALL restricts passage and redirect the traveler to travel document 2nd level of inspection.		
REQ 84.	Following MRZ configurations MUST be supported: • 44*2 symbols; and • 30*3 symbols.		

5.1.3 RFID CHIP READER

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 85.	Reading of chips compliant to ISO 14443 Type A and B, LDS 1 and LDS 2 defined in [ICAO9303] Part 10 MUST be supported.		
REQ 86.	Transmission protocol T=CL MUST be supported.		
REQ 87.	Data exchange rates 106, 212, 424 and 848 kbps MUST be supported.		
REQ 88.	Support of VHBR Data exchange rates up to 6.78Mb/s is RECOMMENDED.		
REQ 89.	Chip detection in any part of the document MUST be supported.		
REQ 90.	Chip MUST be readable when TD1 or TD3 document is positioned on the optical reading surface.		
REQ 91.	Anti-collision protocol (chip selection based on MRZ or CAN reading results) MUST be used.		

5.1.4 CERTIFICATION AND COMPLIANCE OF THE DOCUMENT READER

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 92.	Document readers MUST have the following certifications - CE, RoHS.		
REQ 93.	Document readers MUST have the following certifications: [EN 62368-1], [EN62471].		
REQ 94.	The RF-reading module MUST be certified according to [TR 03105-4]		
REQ 95.	The document reader MUST comply with the existing regulations regarding EMC and UV-A light emissions.		

5.1.5 PERFORMANCE CAPABILITIES AND TEMPORAL REQUIREMENTS

No.	Requirement Description	VENDOR'S RESPONSE	Fulfilled
REQ 96.	On average, optical images of the MRZ MUST be captured within 2 seconds		
REQ 97.	Content of the extracted DG1 MUST be made available in ≤ 5 seconds[1] after the document[2]: • has been placed onto the reader; or • fixed in reading position.		
REQ 98.	Document verification MUST start as soon as the input data becomes available to the system.		
REQ 99.	Full document verification process of an electronic MRTD[3] SHALL NOT take longer than 7 seconds[4].		

5.1.6 COMMUNICATION REQUIREMENTS FOR THE RF-READING MODULE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 100.	The RF-reading module SHALL communicate with a semi-conductor device in the electronic MRTD using radio frequency energy that meets the requirements specified in [ISO 14443]		

[1] Corresponds to t_1 on the Figure 11.
[2] Estonian passport of 2014 is used as the Reference electronic MRTD.
[3] On a Reference electronic MRTD using an Inspection System operated on technology using the minimal system requirements as specified by the manufacturer. [4] Corresponds to t2 on the Figure 11.

5.1.7 CHIP APPLICATION SUPPORT

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 101.	Applications to be supported: • e-Passport (DG01 – DG16); • e-ID (DG01 – DG21); • DTC-PC (DG01 – DG24) and • LDS2 (TravelRecords, VisaRecords, AddBiometrics)		

5.1.8 AUTOMATION REQUIREMENTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 102.	Automatic detection of document placing MUST be supported.		
REQ 103.	Document scanning process MUST start automatically		
REQ 104.	Technical solutions enhancing reading quality of the MRTDs are RECOMMENDED.		

5.2 IMAGE CAPTURE CAMERAS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 105.	The minimum physical resolution of facial image capture camera located at the first door MUST be at least 2 megapixels.		
REQ 106.	The minimum physical resolution of facial image capture camera which is located at the second door MUST be at least 8 megapixels.		
REQ 107.	The camera systems SHALL adapt automatically to the height of the person standing in front of it.		
REQ 108.	The camera systems SHALL cover at least a range of 140cm to 210cm of a person's body height (if standing in marked position in front of the camera system).		
REQ 109.	The camera SHALL be able to capture a full frontal face image, specified in [ISO/IEC 19794-5:2011], of the person if the person is looking straight to the image capture camera without tilting a head.		

REQ 110.	The camera system SHALL guarantee sharpness of the captured facial image if the traveler is positioned within the designated capture area.		
REQ 111.	The camera system SHALL minimize distortion of the captured facial image within the whole capture area.		
REQ 112.	The camera system SHALL be designed to be placed in the moving direction of the traveler.		
REQ 113.	Necessary rotation of the person SHALL be less than 15 degrees		
REQ 114.	The camera system SHALL provide live stream for traveler on instruction screen and guidance for the traveler.		
REQ 115.	If the person is looking straight to the traveler instruction screen the viewing direction of the person SHALL be frontal.		
REQ 116A.	The facial images provided by the capture unit MUST have at least 250 pixels between the centres of the eyes.		
REQ 116B.	Image synthesis based on images from different cameras is not accepted, captured face images MUST be originating from 1 (one) camera device.		
REQ 116C.	The technical tolerance for determining the vertical tilt angle (pitch) of the face plane and the capture of facial image with a camera must remain below 2 degrees.		

5.3 REQUIREMENTS TO THE CAMERA IMAGE QUALITY

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 117.	Uncompressed camera image data for biometric checks SHALL be used.		
REQ 118.	Color depth of facial image processed MUST be 24-bit RGB.		
REQ 119.	Image captured with second door camera MUST fully comply with the EU COMMISSION IMPLEMENTING DECISION (EU) 2019/329 laying down the face image quality requirements.		
REQ 120.	Framed image output resolution for second door camera MUST be 1600x1200.		

5.4 REQUIREMENTS TO THE CAMERA IMAGE QUALITY ASSURANCE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 121.	Pre-qualification of captured live facial images from the acquisition stream MUST be used.		
REQ 122.	Capturing of images other than live facial – for example on the shirt – MUST be avoided.		
REQ 123.	Ranking of images according to the conducted prequalification SHALL be used.		
REQ 124.	Images SHALL be passed to the verification stage as indicated by the rank.		
REQ 125.	Pre-qualification SHALL be conducted at least according to the following criteria: • Absence of multiplicity of faces in the picture; • pose of the head; • illumination of the face; • position of the eyes.		

5.5 LIGHTING

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 126.	Active diffuse lighting SHALL be used to ensure uniform illumination of the captured facial image and to be independent of external lighting.		
REQ 127.	The lighting SHALL NOT cause reflections on glasses or the skin of the face with in the meaning of [ISO/IEC 19794-5:2011].		
REQ 128.	The lighting MAY be active during the complete capture process and brightness MAY be varied to get best contrast and illumination.		

5.6 TABLET

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 129.	The screen size MUST be ≥11" to <14".		

REQ 130.	The screen ratio of the tablet MUST be 9 to 16 or 4 to 3		
REQ 131.	The screen MUST be touch sensitive.		
REQ 132.	The screen brightness MUST be at least 500 cd per sq. m.		
REQ 133.	Battery runtime MUST be at least 8 hours.		
REQ 134.	The tablet orientation in dock during charging MUST be portrait.		
REQ 135.	The tablet MUST have 5G and Wi-Fi connectivity.		
REQ 136.	The tablets MUST have iPadOS 26 or later version operating system.		
REQ 137.	The tablets MUST support at least WPA3 Wi-Fi encryption.		

6 REQUIREMENTS TO THE DOCUMENT READING AND VERIFICATION PROCESSES

Chapter 6 describes data processing procedures that MUST be performed during MRTD inspection process.

All individual document checks as defined in this Technical Specification are applicable to the document under inspection, are mandatory if not otherwise clearly marked, SHALL be performed and SHALL be used in composing requests to PIKO. Checks to which 'undetermined' result would be applicable will not be conducted.

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 138.	Unique monotonously increasing identification number MUST be attributed to every individual document check transaction.		
REQ 139.	Other principles than those provided in RFC 4122 MAY be used for document check transaction numbering.		
REQ 140.	All travelers whose document check aggregate result will not be 'successful' MUST be redirected to manual document check. Corresponding guidance SHALL be displayed on the traveler's screen interface		
REQ 141.	Full document check MUST be performed even if document check aggregate result will not be 'successful'.		

6.1 VISUALISATION OF CHECK RESULTS

The system MUST be able to provide the results of an individual check with reduced level of detail to the operator's desktop workstation and mobile UI. It is RECOMMENDED to map the defined values in the form of traffic lights as shown in table 7.

Result of the check	Traffic light color
Successful	green
Failed	red
Undetermined	yellow
Not supported	grey
Aborted	black

Table 7: Visualization of check results

6.2 WORKFLOW

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 142.	Data in VIZ SHALL NOT be used for document optical checks.		
REQ 143.	For every check the result SHALL be mapped to: • Successful – The check terminated, the feature of the document to be checked successfully passed the check, i.e. a specific check had been able to be applied to the document and assessed according to its specifications. • Failed – The check terminated, the feature of the document to be checked did NOT successfully pass the check; in other words, the applied check failed on the feature. The document SHOULD be subjected to a further (manual) check for authenticity, integrity and validity. • Undetermined – The check terminated, it was not possible to determine if the feature to be checked is authentic, of integrity or is valid.; • Not supported – The check terminated, but the specific document does not support the features to be checked (for example, a document without a chip, a document which does not have specific security features per definition, a specific protocol was not supported by a chip etc.); or Aborted.		
REQ 144.	Any anomaly MUST be considered as an indicator of a possible risk situation resulting in mapping the check to aggregate result 'failed'.		

6.3 CHECKS TO BE CONDUCTED IN COURSE OF THE TRANSACTION PROCESS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 145.	Optical checks MUST be performed.		

REQ 146.	Electronic checks MRZ MUST be performed.		
REQ 147.	Biometric checks MUST be performed.		
REQ 148.	Combined checks MUST be performed.		
REQ 149.	Requests into background systems MUST be performed.		

6.4 PROCESS SEQUENCE OF CHECKING A MRTD

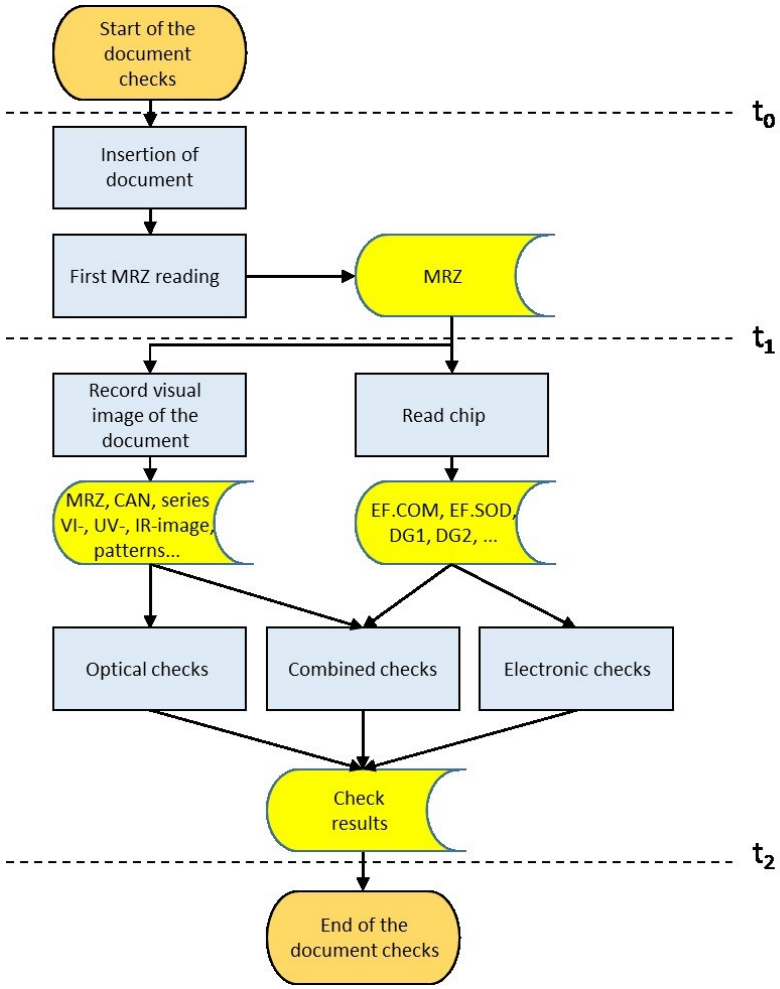

Figure 11. Process sequence of checking MRTDs

Document access MUST start automatically at time t_0 with placing a document to the reader's reading surface. The first reading of the MRZ takes place while the document is slided towards the final reading position. As the MRZ is read while sliding the document to its final reading position, the result of the reading will be available right after the successful result of OCR (time t_1). Fast MRZ allows start PIKO decision making processes as soon as possible. This allows to start communication between the chip and the reader and thus document verification process earlier and reduce overall time of the DG1 and DG2 extraction process for the holder this way increasing throughput of persons.

Upon receiving the results of three checks: 1) background check from PIKO, 2) document optical and electronic check plus 3) result of biometric verification the OK/NOK results of these three

checks will be sent to log servers and decision of opening the gate (Boolean AND) will be made at time t_2.

Time t_3 indicates the moment when, depending on the results of these three checks, the gate will be opened, or the traveler will be asked to wait for assistance. Time delay between making of the gate opening decision and actual action is reserved for decision override by the gate operator. If there is not any override of the decision by the gate operator the gate opening decision will be executed.

After time t_3 information about whether actual border crossing through the gate took place or not will be sent to PIKO.

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 150.	Compatibility with the scheme on Figure 11 MUST be followed.		
REQ 151.	Fast MRZ functionality MUST be supported.		
REQ 152.	Fast MRZ functionality MUST enable you to finish reading MRZ within 1 second after travel document reaching its final reading position.		

6.5 DOCUMENT MODEL

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 153.	Each MRTD MUST be assigned to a document model (sometimes also called series) according to [BSI TR-03135-1] p.5.5.1.1.[4]		

6.6 DOCUMENT MODEL IDENTIFICATION

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 154.	Automatic recognition of a document type and mapping to the document model for all further model specific checking steps.		
REQ 155.	Document model identification MUST be based on the MRZ.		

[4] A document model is defined by means of the country code (C), document type (T), a distinct identification number (N) and a year value (Y).

REQ 156.	Parametrization of the UV recording conditions MUST also be performed based on model identification.		
REQ 157.	Identification of the document model based on model mark on the document MUST be supported.		

6.7 OPTICAL CHECKS

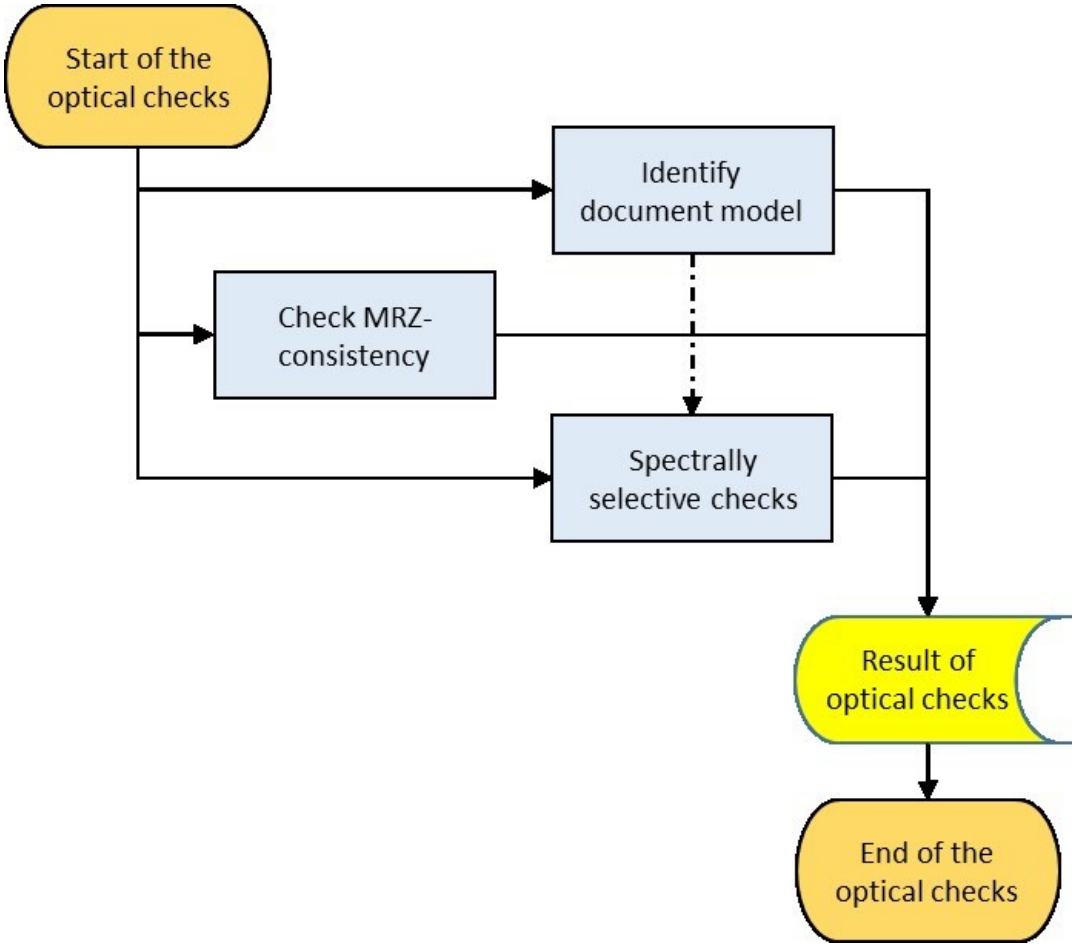

Figure 12. Principal process sequence of optical checks.

6.7.1 REQUIREMENTS TO THE OPTICAL CHECK PROCEDURES

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 158.	Compatibility to the schema on Figure 12.		
REQ 159.	Presence of barcode and contents of decoded barcode data MUST be delivered to ABC gate software.		
REQ 160.	Transliteration of characters in compliance with [ICAO9303] for comparison with MRZ MUST be supported.		

REQ 161.	Optical checks must be performed according to [BSI TR-03135-1] p. 4.4.3.1 and 4.4.3.2.		
REQ 162.	MRZ contents MUST be read in IR light.		
REQ 163.	MRZ contents MUST be read in VI light.		
REQ 164.	CAN contents MUST be read in IR light.		
REQ 165.	CAN contents MUST be read in VI light.		
REQ 166.	Optical quality (i.e. printing clearness etc.) of the MRZ MUST be checked.		
REQ 167.	MRZ (CAN) contents SHALL be OCRed.		
REQ 168.	Positioning of the MRZ according to [ICAO DOC] Part 4 p.3 Figure 3 in bounding rectangle limits MUST be verified.		
REQ 169.	Consistency of MRZ MUST be checked.		
REQ 170.	Syntax of MRZ MUST be checked.		
REQ 171.	Integrity of MRZ MUST be checked.		
REQ 172.	MRZ consistency, syntax and integrity checks MUST be performed on basis of the result of IR OCR.		
REQ 173.	Accuracy of MRZ filling-in MUST be verified.		

6.7.2 SPECTRALLY SELECTIVE CHECK ROUTINES

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 174.	Local document model database assisting in the checking process.		
REQ 175.	Assignment of an unique identifier (UUID according [RFC4122]) for each generic check by the manufacturer according to [BSI TR-03135-1] p.5.5.1.2		

Feature / Area (ZZ)		**Light Source (XX)**		
		VI	UV	IR
Fibers	FI		LU	
Full data page	FU		BR	

Static printed feature	IS	{AB, TR}	LU	{AB, TR, TL}
MRZ	MR	AB	BR	AB
Overprinted MRZ	OM		LU	
CAN	CA	AB		AB
Personalized perforation (dynamic)	PD	AB	LU	AB
Perforation of the substrate	PS	AB	LU	AB
Photo	PH	{AB, FR}	{BR, FR}	{AB, FR, TR}
Secondary Photo	SP	{AB, TR}	LU	{AB, TR}
Overprinted photo	OP		LU	
Security thread	TH	TR	LU	AB
Visual Inspection Zone (VIZ)	VZ		BR	
Watermark	WM			AB
Personalized dynamic feature	ID	{AB, TR}	LU	{AB, TR}
Additional feature	AF	{AB, BR, LU, TL, TR}	{AB, BR, LU, TL, TR}	{AB, BR, LU, TL, TR}

Table 8: Matrix representation of the generic basic check routines.

Used abbreviations according to the [BSI TR-03135-1] p.5.5.1.2.

In addition, there can be the following composite check routines:

– (**IR, AB, TH**) in combination with (**VI, TR, TH**): Check that a thread visible under IR light is invisible under white light.

– (**IR, TR, ID**) in combination with (**VI, AB, ID**): Check that the ink of the dynamic print image absorbent under white light is transparent under IR light.

– (**IR, TR, IS**) in combination with (**IR, AB, IS**): Check that some parts of the static print image are absorbent under IR light, whereas other parts of the characteristics are transparent.

– (**IR, TR, IS**) in combination with (**VI, AB, IS**): Check that the ink of the static print image absorbent under white light is transparent under IR light.

– (**IR, TR, IS**) in combination with (**VI, AB, IS**) and (**IR, AB, ID**): Check that the ink of the static print image absorbent under white light is transparent under IR light and a dynamically printed characteristic becomes visible in the same position under IR light.

6.7.3 CLASSIFICATION AND LOGGING CHECK ROUTINES

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 176.	Classification and logging of manufacturer- and model-specific check routines according to the schema given in Table 8.		

6.7.4 CATALOGUE FOR SPECTRALLY SELECTIVE CHECKS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 177.	Supporting a catalogue according to [BSI TR-03135-1] p. 5.5. 1.3		
REQ 178.	Presence of the following information on each generic check routine of a document model: • UUID of the check routine; • Generic check identifier; • Proprietary check; • Textual description of the check routine performed; • Attribute containing the upper limit of the range of values; • Attribute containing the lower limit of the range of values; • Attribute containing the threshold configured for the decision for the spectrally selective verification; • The bounding rectangle for the checking area; or • The description of an alternative geometric check region if a bounding rectangle is not applicable; • The image section of the reference image region checked against the corresponding database.		
REQ 179.	Any proprietary decision function for composite generic check routines MUST be described by the manufacturer and disclosed to the Contracting Authority.		
REQ 180.	Listing of all test configurations with group checks and decision functions for the given document models.		

6.8 ELECTRONIC CHECKS OF MRTDS

6.8.1 SUPPORT OF THE FOLLOWING ALGORITHMS, PROTOCOLS AND SECURITY MECHANISMS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 181.	DH and ECDH key agreement algorithms MUST be supported.		
REQ 182.	BAC according to [ICAO9303] Part 11 MUST be supported.		
REQ 183.	PACE according to [ICAO9303] Part 11 MUST be supported.		
REQ 184.	PA according to [ICAO9303] Part 11 MUST be supported.		
REQ 185.	AA according to [ICAO9303] Part 11 MUST be supported.		
REQ 186.	Terminal Authentication (TA v1, TA v2) MUST be supported.		
REQ 187.	Chip Authentication (CA v1, CA v2) MUST be supported.		

6.8.2 FILES AND DATA GROUPS TO BE SUPPORTED

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 188.	EF.COM		
REQ 189.	EF.SO_D V1		
REQ 190.	EF.SO_D V2		
REQ 191.	DG11		
REQ 192.	DG12		
REQ 193.	DG13		
REQ 194.	DG14		
REQ 195.	DG15		
REQ 196.	EE.CVCA		
REQ 197.	EF.CardAccess		
REQ 198.	EF.CardSecurity		

REQ 199.	EF.ChipSecurity		
REQ 200.	DG1		
REQ 201.	DG2		
REQ 202.	DG3		

6.8.3 CHIP ACCESS USING BAC OR PACE PROTOCOLS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 203.	It MUST be possible to configure the system in order that PACE will be used as the primary protocol and BAC will be used as the fallback one in case corresponding document model defines support of both protocols.		
REQ 204.	The inspection system SHALL not use both – BAC and PACE in the same session if fallback is not required.		
REQ 205.	The result of chip MUST be mapped regarding the following list: • Successful – The result of chip access MUST be set to 'successful' if access protocol used as referenced in the profiling as mandatory has been successful. Also, the result is set to 'successful' if the primary protocol fails but secondary protocol succeeds if fallback has been allowed in document model. • Failed – The result of chip access MUST be set to 'failed' if access protocol used as referenced in the profiling as mandatory has been rated as failed. • Unsupported - The result of chip access MUST be set to 'unsupported' if neither BAC nor PACE could be performed to access the document. • Aborted – The result of chip access MUST be set to 'aborted' if due to an error the access process was aborted prior to its defined process flow.		

6.9.4 CHIP ACCESS VIA BAC

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 206.	The result of checking of the chip access by BAC MUST be mapped regarding the following list: • Successful – The result of the check must be set to 'successful' if BAC could be performed successfully. • Failed – The result of the check must be set to 'failed' if CA was performed, but performing of the protocol failed, the secure messaging channel could not be established successfully. • Not supported – The result of the check must be set to 'not supported' if it is not necessary to perform BAC in order to access the document (the document might also be accessed with an unencrypted channel or using PACE). • Aborted – The result of the check MUST be set to 'aborted' if due to an error the check was aborted prior to its defined process flow.		

6.9.5 CHIP ACCESS VIA PACE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 207.	The result of checking of the chip access by PACE MUST be mapped regarding the following list: • Successful – The result of the check must be set to 'successful' if PACE could be performed successfully. • Failed – The result of the check must be set to 'failed' if CA was performed, but performing of the protocol failed, the secure messaging channel could not be established successfully. • Not supported – The result of the check must be set to 'not supported' if it is not necessary to perform PACE in order to access the document (the document might also be accessed with an unencrypted channel or using BAC). • Aborted – The result of the check MUST be set to 'aborted' if due to an error the check was aborted prior to its defined process flow.		

6.9.6 CHECKING CHIP ACCESS BY TERMINAL AUTHENTICATION (TA)5

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 208.	The result of checking of the chip access by TA MUST be mapped regarding the following list: • Successful – The result of the check must be set to 'successful' if PACE could be performed successfully. • Failed – The result of the check must be set to 'failed' if CA was performed, but performing of the protocol failed, the secure messaging channel could not be established successfully. • Not supported – The result of the check must be set to 'not supported' if it is not necessary to perform PACE in order to access the document (the document might also be accessed with an unencrypted channel or using BAC). • Aborted – The result of the check MUST be set to 'aborted' if due to an error the check was aborted prior to its defined process flow.		

6.9.7 CHECKING THE CHIP AUTHENTICITY (AA, CA)

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 209.	The system MUST support altering the chip authenticity checking algorithm sequence.		
REQ 210.	CA is RECOMMENDED to be used if both protocols (CA and AA) are supported by the document chip.		

[5] Will be applicable only after implementation of EAC

REQ 211.	The result of checking of the chip authenticity MUST be mapped regarding the following list: • Successful – The result of checking of the chip authenticity MUST be set to 'successful' if AA or CA could be performed successfully. • Failed – The result of checking of the chip authenticity MUST be set to 'failed' if both protocols were performed and both failed, or both protocols were performed and one failed and the other was not successful, or only one was performed and failed. • Undetermined – The result of the check must be set to undetermined if, by means of both protocols, checking the authenticity of the chip could not be determined with either AA or CA (e. g. missing data/information for the check). • Not supported – The result of the check must be set to not supported if AA and CA were tried but could not be executed on a particular document. • Aborted – The result of checking of the chip authenticity MUST be set to 'aborted' if due to an error the checking process was aborted prior to its defined process flow.		
REQ 212.	If only one of the checks from pp. 6.9.8 and 6.9.9 is 'not supported' and the other one is 'successful' or 'failed' the result is 'successful' or 'failed'. If both results are 'not supported' the result is also 'not supported' and the traveler MUST be redirected to manual inspection.		

6.9.8 CHECKING CHIP AUTHENTICITY WITH AA

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 213.	The result of checking of the chip authenticity with AA MUST be mapped regarding the following list: • Successful – The result of the check must be set to 'successful' if AA could be performed successfully. • Failed – The result of the check must be set to 'failed' if AA was performed, but performing of the protocol failed, although the required data and parameters required for AA are available. • Undetermined – The result of the check must be set to 'undetermined' if the result of checking of the authenticity of the chip cannot be determined. • Not supported – The result of the check must be set to 'not supported' if AA was tried but could not be executed. • Aborted – The result of the check MUST be set to 'aborted' if due to an error the check was aborted prior to its defined process flow.		

6.9.9 CHECKING CHIP AUTHENTICITY WITH CA

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 214.	The result of checking of the chip authenticity with CA MUST be mapped regarding the following list: • Successful – The result of the check must be set to 'successful' if CA could be performed successfully. • Failed – The result of the check must be set to 'failed' if CA was performed, but performing of the protocol failed, although the required data and parameters required for CA are available. • Undetermined – The result of the check must be set to 'undetermined' if the result of checking of the authenticity of the chip cannot be determined. • Not supported – The result of the check must be set to not supported if CA was tried but could not be executed. • Aborted – The result of the check MUST be set to 'aborted' if due to an error the check was aborted prior to its defined process flow.		

6.9.10 CHECKING THE ELECTRONIC DATA AUTHENTICITY WITH PASSIVE AUTHENTICATION (PA)

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 215.	C_{DS} authenticity may be confirmed only either by local ML deliverable by the CA or via TCC PA service (see Figure 5).		

6.9.11 VERIFICATION OF THE SECURITY OBJECTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 216.	Ability to process security objects with one, several or no C_{DS} MUST be supported.		
REQ 217.	Verification of the hash and signature for EF.CardSecurity and mapping to its own final check result (if existing) MUST be performed.		
REQ 218.	Verification of the hash and signature for EF.ChipSecurity and mapping to its own final check result (if existing) MUST be performed.		
REQ 219.	Verification of the hash and signature for $EF.SO_D$ and mapping to its own final check result MUST be performed.		
REQ 220.	Verification of the digital signature of a security object MUST be performed.		
REQ 221.	Comparison of the stored and calculated on site security object's hash values MUST be performed.		
REQ 222.	If EF.COM is present in the e-Passport chip (in addition to $EF.SO_D$), the content of EF.COM with $EF.SO_D$ MUST be compared to assure that each DG listed in $EF.SO_D$ is also contained in EF.COM and vice versa.		

REQ 223.	The result of checking the security objects MUST be mapped regarding the following list: • Successful – The result of checking of the security objects MUST be set to 'successful' if all checks from this subsection referenced in the profiling as mandatory were checked as successful. • Failed – The result of checking of the security objects MUST be set to 'failed' if at least one of the checks from this subsection that were referenced in the profiling, is rated as failed. • Undetermined – The result of the check must be set to undetermined if information is missing to perform the verification. • Aborted – The result of checking of the security objects MUST be set to 'aborted' if due to an error the checking process was aborted prior to its defined process flow.		

6.9.12 CHECKING ISSUER CERTIFICATES

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 224.	Check of the issuer certificate for EF.SO_D MUST be performed.		
REQ 225.	Check of the issuer certificate for EF.CardSecurity MUST be performed.		
REQ 226.	Check of the issuer certificate for EF.ChipSecurity MUST be performed.		
REQ 227.	Check of C_{DS} signature against its respective C_{CSCA} MUST be performed.		
REQ 228.	Check if the document inspection time is within the validity period of the C_{DS} MUST be performed.		
REQ 229.	Check of the revocation state of the C_{DS}[6] MUST be performed.		
REQ 230.	Trust Status MUST be assessed to the Certificates.		

[6] In case when in the C_{DS} verification service (See Figure 5) has been implemented.

REQ 231.	The cumulative result of checking of the issuer certificates MUST be mapped regarding the following list[7]: • Successful – The result of checking of the issuer certificates MUST be set to 'successful' if all checks from this subsection referenced in the profiling as mandatory were checked as successful. • Failed – The result of checking of the issuer certificates MUST be set to 'failed' if at least one of the checks from this subsection that were referenced in the profiling, is rated as failed. • Undetermined – The result of the check must be set to undetermined if information is missing for performing the check. • Aborted – The result of checking of the issuer certificates MUST be set to 'aborted' if due to an error the checking process was aborted prior to its defined process flow.		
REQ 232.	In case the cumulative result of checking the issuer certificates is not set to 'successful' the traveler SHALL be redirected to manual inspection.		

6.9.13 CHECKING INTEGRITY OF CHIP CONTENTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 233.	Check whether each data group listed in $EF.SO_D$ is also included in EF.COM MUST be performed.		
REQ 234.	Integrity check of all data groups MUST be performed.		
REQ 235.	Integrity check of each individual data group MUST be performed.		
REQ 236.	The result of checking of the integrity of chip content MUST be mapped regarding the following list: • Successful – The result of checking of the integrity of chip contents MUST be set to 'successful' if all checks from this subsection referenced in the profiling as mandatory were checked as successful. • Failed – The result of checking of the integrity of chip contents MUST be set to 'failed' if at least one of the checks from this subsection that were referenced in the profiling, is rated as failed. • Aborted – The result of checking of the integrity of chip contents MUST be set to 'aborted' if due to an error the checking process was aborted prior to its defined process flow.		

[7] Status 'trusted' is considered equal to the status 'successful'

6.9.14 COMPARING EF.S_{OD} WITH EF.COM

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 237.	Check whether each data group listed in EF.S_{OD} is also included in EF.COM MUST be performed.		
REQ 238.	The result of comparing EF.S_{OD} with EF.COM MUST be mapped regarding the following list: • Successful – The result of the check must be set to 'successful' if the contents of EF.COM and EF.S_{OD} are consistent with each other. • Failed – The result of the check must be set to 'failed' if inconsistencies between EF.COM and EF.S_{OD} were detected. • Not supported – The result of the check must be set to 'not supported' if comparing the contents of EF.S_{OD} and EF.COM is not possible, e. g. because one or both files are not on the document. • Aborted – The result of comparing EF.S_{OD} with EF.COM MUST be set to 'aborted' if comparing EF.S_{OD} and EF.COM was aborted due to an error.		

6.9.15 CHECKING DATA GROUP INTEGRITY

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 239.	For each data group which was read from the chip, the hash value SHALL be calculated and compared to the corresponding hash value given in EF.S_{OD}.		

REQ 240.	The result of checking data group integrity MUST be mapped regarding the following list: • Successful – The result of the check must be set to 'successful' if the result of the check must be set to successful if all mandatory (regarding the profiling) data groups to be checked, were read and the calculated hash values were identical. • Failed – The result of the check must be set to 'failed' if one or more data group integrity checks result in not identical. • Undetermined – The result of the check must be set to 'undetermined' if the result is neither 'successful' nor 'failed'. • Aborted – The result of comparing EF.S_{OD} with EF.COM MUST be set to 'aborted' if building the result or an underlying, specific check was aborted.		

6.9.16 COMPARISON OF THE ISSUING STATE (DG1 AND DS CERTIFCATE)

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 241.	Comparison of the issuing country (country codes in DG1 and C_{DS}) MUST be performed.		
REQ 242.	The result of comparison of the issuing country MUST be mapped regarding the following list: • Successful – The result of the check must be set to 'successful' if the ICAO country code and the ISO country code match each other based on the information in the assignment table. • Failed – The result of the check MUST be set to 'failed' if the ICAO country code and the ISO country code do not match each other based on the information in the assignment table. • Undetermined – The result of the check MUST be set to 'undetermined' if information is missing to perform the check. • Aborted – The result of comparing EF.S_{OD} with EF.COM MUST be set to 'aborted' if comparison of the issuing states was aborted.		

6.10 COMBINED CHECKS

6.10.1 CROSS VERIFICATION OF MRZ DATA

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 243.	Cross-verification of data retrieved from MRZ and DG1 of the RFID chip MUST be performed.		
REQ 244.	Cross-verification of MRZ data SHALL be performed comparing OCR results of (IR, AB, MR), (VI, AB, MR) and DG1.		
REQ 245.	The result of MRZ cross verification check MUST be mapped regarding the following list: • Successful – The result of the check MUST be set to 'successful' if all instances of MRZ match. • Failed – The result of the check MUST be set to 'failed' if at least one instance of MRZ differs from the other two. • Aborted – The result of the check MUST be set to 'aborted' if due to an error the checking process was aborted prior to its defined process flow.		

6.10.2 VERIFICATION OF DOCUMENT VALIDITY

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 246.	Verification of MRTD validity based on retrieved information from MRZ MUST be performed.		
REQ 247.	The result of document validity verification check MUST be mapped regarding the following list: • Successful – The result of the check MUST be set to 'successful' if the date of verification is within validity period of the MRTD. • Failed – The result of the check MUST be set to 'failed' if the date of verification is outside of validity period of the MRTD. • Aborted – The result of the check MUST be set to 'aborted' if due to an error the checking process was aborted prior to its defined process flow.		

6.11 BIOMETRIC CHECKS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 248.	Detailed Acquisition and Comparison Workflows MUST be used for all use cases described in P.1		
REQ 249.	Reference image SHALL be acquired from the DG2 of the travel Document, DTC Type 1 local temporary buffer or from DTC Type 2.		
REQ 250.	Comparison of holder's facial image in the DG2 to the live image collected from the image capture camera MUST be performed.		
REQ 251.	PAD detection MUST be supported by the camera solution. The gate operator should ensure that the document holder does not try to illegally bypass the border control by using fake biometrics or other mechanisms when a spoofing attack (PAD) is detected.		
REQ 252.	Morphing Attack Detection (MAD) MUST be supported by the ABC Gates solution. The ABC Gates operator should ensure that the document holder does not try to use morphed image in travel Document for the border crossing.		
REQ 253.	The result of comparison of holder's facial images MUST be mapped regarding the following list: • Successful – The result of comparison of holder's facial images MUST be set to 'successful' if the images match each other. • Failed – The result of comparison of holder's facial images MUST be set to 'failed' if the images do not match each other, specified time-out has reached or when a spoofing attack (PAD) is detected. • Undetermined – The result of comparison of holder's facial images MUST be set to 'undetermined' if information is missing to perform the check when specified time-out has reached. • Aborted – The result of comparison of holder's facial image MUST be set to 'aborted' if comparison of holder's facial images was aborted.		

6.12 REQUIREMENTS TO THE BIOMETRIC COMPARISON

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 254.	The face extraction algorithm security level (threshold) to obtain different values of FTA and FTE MUST be configurable.		

REQ 255.	The ABC Gates Service provider MUST provide calibration data based on the actual verification performance.		
REQ 256.	The output of the algorithm SHALL be a comparison score[8] 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.		
REQ 257.	The ABC Gates Service provider SHALL provide a DET curve of algorithm performance.		
REQ 258.	Such performance SHALL be based on images of comparable characteristics (e.g. images in size and resolution and pose variation of a typical ePassport deployment).		
REQ 259.	Face matching algorithm MUST have FNMR =< 0.002 @ FMR = $10^{-6.}$		
REQ 260.	Face matching algorithm MUST be tested by NIST or an organization with equivalent competence using the same methodology.		

6.13 REQUIREMENTS TO THE PRESENTATION ATTACK DETECTION

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 261.	The PAD solution MUST be evaluated by independent third party according to ISO/ ISO/IEC 30107-3.		
REQ 262.	The PAD solution MUST have APCER < 0.01 @ BPCER = 0.03.		
REQ 263.	The ABC Gates Service provider must ensure that the PAD measures, APCER and BPCER rates will be kept up to date with regards to advances in the threat landscape, developing risks and available technology.		

[8] Typically, a vendor-specific uncalibrated raw score.

7 ERROR CODES AND LOGGING

7.1 TRANSACTION LOGGING

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 264.	No personal, document or border crossing procedure information is stored or logged in the ABC gates. All data except personal, document or border crossing procedure information obtained during a document inspection process SHALL be stored according to the monitoring logdata format.		
REQ 265.	The following global states of an inspection process will be logged: • Successful • Terminated Aborted		
REQ 266.	The result of an inspection process will be logged: • Successful • Failed • Undetermined • Not supported Aborted		
REQ 267.	Processing errors of each of the checks prescribed in this Technical Specification resulting in an aborted check MUST be logged together with timestamp and gate unique identifier.		
REQ 268.	System error codes together with timestamp and unique gate identifier MUST be logged. These errors can be but not limited to: • MRZ IR reading error; • MRZ OCR error; • document validity error; • Chip communication error; • Chip authenticity error; • MRZ or CAN reading error; • BAC or PACE accomplishment error; • CA1/CA2 error; • defect Document Signer Certificate Revoked (BSI TR-03129-2, 4.2.1.1) is detected for a CDS; other document verification process errors.		

REQ 269.	Error code message syntax MAY be specified by the ABC Gates Service provider, will be agreed with the Contracting Authority and SHALL contain at least following items: • error code; • gate unique identifier; and timestamp.		
REQ 270.	Each error code MUST be in unique numeric integer format number. Return code consists of confirmation of successful operation or error code. Return code of a successful operation is 0 (zero). Database of error descriptions provides a short and concise error description that facilitates a subsequent analysis regarding the error. Database of error descriptions is kept in the management server.		
REQ 271.	Logging of all relevant check results which are provided by the interface specified in Chapter 7 of this Technical Specification MUST be supported.		
REQ 272.	Individual checks MUST be stored in the Management server log.		
REQ 273.	At least following information shown below MUST be included in a data entry: • Total transaction time (document authentication, biometric verification, background checks, etc.); • Total access time; • Issuing country; • Date of issue; • Information about the read document (document type and issuing state) • Travel document model indicator; • Outcome of each of the authentication checks actually performed in the document, depending on the type of document; • Error type and messages from the particular process steps and document reader unit;		

REQ 274.	Within biometric verification workflow, the following data SHALL be collected: • A unique transaction identifier of the current verification process (distinguishable for every verification attempt during the whole border control process) • A Test Flag • A time stamp of the verification process • Information about the duration of the whole process. • Gate unique identifier • Error Code • Information about the loaded reference image (image type and image format) • Duration of capture • For each captured image used for a verification attempt: o Duration of the verification o Configured threshold of the verification software o Result of the genuine comparison (result, score and achieved FMR) o Result of the PAD (result, score) o Result of the MAD (result, score)		
REQ 275.	Events of tailgating and passing the gate in wrong direction MUST be logged together with timestamp and gate unique identifier.		
REQ 276.	Processing errors of each of the checks prescribed in this Technical Specification resulting in an aborted check MUST be logged together with timestamp and gate unique identifier.		
REQ 277.	Error codes of data communication MUST be logged together with timestamp.		
REQ 278.	Events of overriding successful background check procedure result sent from PIKO MUST be logged.		
REQ 279.	Document reader SHALL be able to provide all the document verification data in a format that is sufficient to build [BSI TR-03135-1] compatible transaction log, according to XML schemas provided in [BSI TR-03135-1] p.6.2. Transaction log MUST contain all data obtained in the document verification process, except personal data of a document holder and the MRTD itself.		
REQ 280.	Document verification transaction log MUST be sent to log server of the Contracting Authority.		

REQ 281.	Biometric verification module SHALL be able to provide all the biometric identification data in a format that is sufficient to build [BSI TR-03121] compatible transaction log, according to XML schemas provided in [TR-03121 Scheme v6.1]. Transaction log MUST contain all data obtained in the biometric identification process, except personal data of a document holder and the MRTD itself.		
REQ 282.	Biometric verification transaction log MUST be sent to log server of the Contracting Authority.		
REQ 283.	Archiving of logs will be agreed with Contracting Authority during execution of the Contract.		

8 DEFECTS

8.1 OPTICAL DEFECTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 284.	If the defect 'Specimen' applies to the checked document, the document SHOULD be identified and marked as specimen. Further passing through the gate SHALL be restricted and the traveler SHALL be instructed to wait for gate operator.		
REQ 285.	If the defect 'Country identifier' applies to the checked document, further passing through the gate SHALL be restricted and the traveler SHALL be instructed to wait for gate operator.		
REQ 286.	If the defect 'MRZ format' defect applies to the checked document, further passing through the gate SHALL be restricted and the traveler SHALL be redirected to 2nd level of inspection.		
REQ 287.	If the defect 'MRZ check digit' defect applies to the checked document, further passing through the gate SHALL be restricted and the traveler SHALL be instructed to wait for gate operator.		
REQ 288.	If the defect 'MRZ non-IR-readability' defect applies to the checked document, further passing through the gate SHALL be restricted and the traveler SHALL be redirected to 2nd level of inspection.		

8.2 ELECTRONIC DEFECTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 289.	In case of electronic defects further passing through the gate SHALL be restricted and the traveler SHALL be instructed to wait for gate operator.		

8.3 BIOMETRIC COMPARISON DEFECTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 290.	In case of biometric verification failure further passing through the gate SHALL be restricted and the traveler SHALL be instructed to wait for gate operator.		

9 DATA/INFORMATION EXCHANGE

9.1 DATA EXCHANGE WITH THE GATE OPERATOR DESKTOP WORKSTATION UI

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 291	Information needed to facilitate the following tasks to be carried out by the operator MUST be supplied: • monitoring the user interface of the ABC application; • display notifications in case of malfunction or situations except successful check or redirection of a traveler to 2nd level of inspection to manage exceptions and make decisions about them.		
REQ 292.	Visual feedback of the verification process SHALL be provided for the gate operator.		
REQ 293	At least both facial images (live and reference) SHALL be displayed to the gate operator.		
REQ 294.	In case of document verification mapping to any other result than 'successful' images of VIZ acquired in IR, VI and UV SHALL be displayed to the gate operator.		
REQ 295.	The (Boolean) result of the verification SHALL be displayed to the gate operator.		

REQ 296.	Manual override command and redirection of a traveler to 2nd level of inspection from the gate operator MUST be supported.		
REQ 297.	The result of the biometric verification process SHALL be provided to the ABC Gates operator's screen.		
REQ 298.	The overall verification result MUST be displayed in the summary view appearing on the ABC Gates operator's screen.		
REQ 299.	The image data (VIZ image, DG2 image and live image used for the verification) MUST be shown in the summary view on the ABC Gates operator's screen.		
REQ 300.	In case of overriding successful control procedure (no border crossing occurred) event MUST be sent to PIKO.		
REQ 301.	Reason for override of unsuccessful control procedure sent from PIKO MUST be displayed on the ABC Gates operator's screen (will be coordinated and agreed with the Contracting Authority).		
REQ 302.	Further details regarding the detailed checks of the biometric verification process SHALL be displayed upon discretion of the gate operator.		
REQ 303.	The result of MRZ optical check and comparison (OK/NOK) MUST be displayed on the ABC Gates operator's screen. Upon discretion of the gate operator detailed information SHALL be displayed.		
REQ 304.	The result of eMRTD data verification (OK/NOK) MUST be displayed on the ABC Gates operator's screen. Upon discretion of the gate operator detailed information SHALL be displayed.		
REQ 305.	A button "Border crossing allowed" for overriding the results of the document /personal identity checks MUST be displayed on the ABC Gates operator's screen. The button MUST be deactivated in case background check 'NOK' decision will be sent from PIKO.		
REQ 306.	The results of background requests to PIKO (OK/NOK) MUST be displayed on the ABC Gates operator's screen. Upon discretion of the gate operator detailed information SHALL be displayed.		
REQ 307.	A button "Send to 2nd level of inspection" together with a selectable list of redirection reasons MUST be activated on the ABC Gates operator's screen in case 'NOK' decision together with list of options will be sent from PIKO.		

REQ 308.	In case of malfunction of data exchange with PIKO a message MUST be displayed on the ABC Gates operator's screen to proceed without redirecting the traveler to 2nd level of inspection if it's needed and/or possible.		
REQ 309.	An alert in case of an attempt to use ABC Gates by a minor MUST be displayed on the ABC Gates operator's screen.		
REQ 310.	An alert in case of a PAD positive result MUST be displayed on the ABC Gates operator's screen.		
REQ 311.	An alert in case of a MAD positive result MUST be displayed on the ABC Gates operator's screen.		
REQ 312.	Alerts MUST be displayed on the ABC Gates operator's screen: • in case of tailgating; • traveler stuck inside ABC gate; • abandoned luggage; • in case of border crossing in wrong direction; • in case of technical malfunction (door stuck, missing communication with document reader, …); • The ABC user is a minor, i.e. between the ages of 12 and 18. • etc. c		
REQ 313.	A notice about a traveller sent to manual control MUST be displayed on the ABC Gates operator's screen.		
REQ 314.	A notice about ABC gate manual override activated MUST be displayed on the ABC Gates operator's screen.		
REQ 315.	The ABC Gates operator desktop workstation UI SHALL be operating in Windows 11 EE environment.		
REQ 316.	The solution of authentication and authorization of the ABC Gates operator desktop workstation UI SHALL be agreed with the Contracting Authority during execution of the Contract.		

9.2 DATA EXCHANGE WITH THE ABC GATES OPERATOR MOBILE UI

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 317.	The overall verification result MUST be displayed in the summary view appearing on the ABC Gates operator's mobile screen.		
REQ 318.	The result of the biometric verification process (OK/NOK) MUST be displayed to the ABC Gates operator's mobile screen. The image data (VIZ image, DG2 image and live		

	image used for the verification) SHALL be displayed as pop-ups upon request by the ABC Gates operator.		
REQ 319.	The result of MRZ optical check and comparison (OK/NOK) MUST be displayed on the ABC Gates operator's mobile screen. Upon discretion of the ABC Gates operator detailed information SHALL be displayed.		
REQ 320.	The result of eMRTD data verification (OK/NOK) MUST be displayed on the ABC Gates operator's mobile screen. Upon discretion of the ABC Gates operator detailed information SHALL be displayed.		
REQ 321.	A button "Border crossing allowed" for overriding the results of the document /personal identity checks MUST be displayed on the ABC Gates operator's screen. The button MUST be deactivated in case 'NOK' decision will be sent from PIKO.		
REQ 322.	The results of background requests to PIKO (OK/NOK) MUST be displayed on the ABC Gates operator's mobile screen. Upon discretion of the ABC Gates operator detailed information and workflow SHALL be displayed.		
REQ 323.	A button "Send to 2nd level of inspection" together with a selectable list of redirection reasons MUST be activated on the ABC Gates operator's screen in case 'NOK' decision will be sent from PIKO.		
REQ 324.	In case of document verification mapping to any other result than 'successful' images of VIZ acquired in IR, VI and UV SHALL be displayed on the ABC Gates operator's mobile screen.		
REQ 325.	An alert in case of an attempt to use a ABC Gates by a minor MUST be displayed on the ABC Gates operator's mobile screen.		
REQ 326.	Alerts MUST be displayed on the ABC Gates operator's mobile screen: • in case of tailgating; • traveller stuck inside gate; • abandoned luggage; • in case of border crossing in wrong direction; • in case of technical malfunction (door stuck, missing communication with document reader, …); etc.		
REQ 327.	A notice about a traveler sent to 2nd level of inspection MUST be displayed on the ABC Gates operator's mobile screen.		
REQ 328.	A notice about ABC gate manual override activated MUST be displayed on the ABC Gates operator's mobile screen.		

REQ 329.	The solution of authentication and authorization of the ABC Gates operator mobile UI SHALL be agreed with the Contracting Authority during execution of the Contract.		

9.3 INSTRUCTIONS FOR A TRAVELLER

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 330.	Full guidance MUST be provided on the ABC gate screen. The contents of the guidance, e.g. looping video, SHALL be coordinated with CA.		
REQ 331.	An indicator showing the capture status SHOULD be displayed to the passenger.		
REQ 332.	Information about whether a ABC gate is operational or not MUST be displayed to the travelers in clear and understandable form.		
REQ 333.	Up to 2 (two) communication languages MUST be specified for a country. Communication language SHALL be derived from the correspondence table according to the country code in the MRZ of a MRTD. The correspondence table MUST be agreed with the PBGB during execution of the Contract.		
REQ 334.	Audio instructions for the traveler MAY be provided.		
REQ 335.	The information for the traveler MUST contain following messages but not limited to: • Information about the successful or failed verification process; • Document removed too early – repeat document reading from the beginning; • Request to wait for assistance; The contents of the list MUST be expandable. The contents and wording SHALL be coordinated with PBGB.		
REQ 336.	Graphics on the traveler's UI screen should avoid multiple colors or harsh contrast.		
REQ 337.	A correspondence table containing system messages and respective messages to the traveler MUST be present in the management server. The contents of this table SHALL be agreed with the Contracting Authority during execution of the Contract.		

9.4 DATA EXCHANGE WITH PIKO

Figure 13. Conceptual PIKO API data exchange sequence diagram.

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 338.	PIKO interface specification SHALL be agreed with the Contracting Authority during execution of the Contract. Conceptual PIKO API data exchange sequence diagram is provided in the Figure 13.		
REQ 339.	The information exchange between the ABC solution and PIKO SHALL take place only via PIKO API.		
REQ 340.	The following data MUST be transmitted to PIKO: • Use cases a, b, d, f, g described in section P.1 - MRZ • Use cases c, e described in section P.1 – MRZ and EES compliant face image and/or 4 fingerprint images. Additionally for all use cases: • The event of real border crossing accomplished. • Border crossing is not accomplished.		
REQ 341.	For every data transfer message sent there MUST be a response in form of return codes. This requirement is applicable to both parties of data transfer. Missing of reply MUST not be considered as proof of successful data transfer.		
REQ 342.	List of data transfer response return codes SHALL be agreed between the Contracting Authority and the ABC Gates Service provider during finalizing the PIKO interface.		
REQ 343.	ABC Gates Service provider MUST develop and hand over PIKO API emulator to Contracting Authority after finalizing the PIKO interface with the aim of enabling testing of the API implementation.		
REQ 344.	Final end-to-end API testing must be performed on test systems before going live with ABC Gates Solution.		

10. MONITORING AND STATISTICAL DATA REPORTING

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 345.	The ABC Service Provider MUST provide remote secure access to ABC Gates solution graphical interfaces that allow displaying ABC gates monitoring data, service		

	statistics, and the data of each ABC gate pass or ABC gate pass attempt.		
REQ 346.	The ABC Solution MUST offer the ability to generate the following types of ad hoc reports: 1. Number of Passthrough - ABC gate-based, with the possibility to select the time frame (incl. successful, aborted etc.); 2. Passthrough analysis – ABC gate-based crossings, with the possibility to select the time frame in the view of failed process components (for ex. General failed, Biometric, Document, Face, Fingerprint, Face PAD, Fingerprint PAD, Face MAD, Tailgating, Penetration, Background, Police search, Aborted etc.) 3. Nationality Passthrough overview – ABC gate-based, with the possibility to select the time frame (incl. total, successful, abort etc.) 4. Nationality Passthrough analysis - with the possibility to select the time frame in the view of failed process components (for ex. General failed, Biometric, Document, Face, Fingerprint, Face PAD, Fingerprint PAD, Face MAD, Tailgating, Penetration, Background, Police search, Aborted etc.) 5. Passenger Statistics – ABC gate-based crossings, with the possibility to select the time frame. Criterias: Age group, Sex, Document type, Nationality. 6. Attempts of ABC gates usage report – ABC gate-based crossings, with the possibility to select the time frame in the view of failed process components (for ex. Total attempts, Total failed, Age rejection, Nationality rejection, Expiry rejection, Incorrect submission, Inspection interrupted, No chip detected, Document type rejection, Other rejection etc.) 7. Attempts of ABC gates usage by Nationality - gate-based crossings, with the possibility to select the time frame in the view of failed process components (for ex. Total attempts, Total failed, Age rejection, Nationality rejection, Expiry rejection, Incorrect submission, Inspection interrupted, No chip detected, Document type rejection, Other rejection etc.) 8. Biometric Evaluation – ABC gate-based, with the possibility to select the time frame (in here matching, PAD, MAD) in views falce accept rate, false rejection rate, score treshold. 9. Duration Statistics – ABC gate-based crossings, with the possibility to select the time frame with the steps on workflow view (for ex. Total min., total avg., total max., doc avg., doc min., doc max., bio min., bio max.,		

	bio avg., fingerp max, fingerp min., fingerp avg., MRZ min., MRZ max., MRZ avg., etc.) 10. Inspection Time Details – ABC gate-based, with the possibility to select the time frame based on Country and Document Type (for ex. doc avg., doc min., doc max., bio min., bio max., bio avg., fingerp max, fingerp min., fingerp avg., MRZ min., MRZ max., MRZ avg., etc.) 11. Document Appearances – based on Country and Document type 12. Document Signer Appearances – (for ex. Subject, Issuer, Hash, Country, First Occurrence, Document Type, BCC, CSCA not found ..etc.) 13. Document Electronic Check overview - with the possibility to select the time frame based on Country and Document type (in here successful, failed) 14. Document Optical Check overview - with the possibility to select the time frame based on Country and Document type etc. (in here successful, failed) 15. Combined Check – chip vs MRZ, VIS etc. with the possibility to select the time frame, based on Country and Document Type (for ex. Successful, failed etc.) 16. Document Optical Check overview - with the possibility to select the time frame based on Country and Document Model etc. (in here successful, failed) 17. ABC gates status overview – ABC gate-based crossings, with the possibility to select the time frame (in here uptime, downtime, active, closed, initializing, error, offline, total time frame, number of restarts etc.).		

11 REQUIREMENTS TO SECURITY OF THE ABC SERVICE

11.1 SOLUTION SECURITY

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 347.	Secure communication between ABC gates, management server and Contracting Authority Information Systems MUST implemented according to Figure 8. „Schematic description of the solution“		
REQ 348.	The ABC Service Provider MUST coordinate the used IP address spaces with the Contracting Authority.		

REQ 349.	ABC Solution implementation MUST not have any access to/from internet.		
REQ 350.	SMIT jump solution MUST be used for access and management of ABC Gates solution.		
REQ 351.	All ABC gates MUST use SMIT LAN-s in ABC gates locations.		
REQ 352.	Mutual authentication MUST be implemented between user applications (ABC Gates operator, monitoring, statistics, etc.).		
REQ 353.	All data MUST be encrypted both during data transit and during temporary storage.		
REQ 354.	All security patches to software and firmware components related to the ABC Gates solution platform, including operating systems, SHOULD be implemented accordingly to [BSI C5:2020] OPS-22 Testing and Documentation of known Vulnerabilities: • Critical (CVSS = 9.0 – 10.0), 3 hours; • High (CVSS = 7.0 – 8.9), 3 days; • Average (CVSS = 4.0 – 6.9), 1 month; and • Low (CVSS = 0.1 – 3.9), 3 months from security patches becoming available. ENISA EU Vulnerability Database MUST be used as source.		
REQ 355.	Transaction logs of ABC Gates Solution consisting of all checks, captures, comparisons and circumstances detected together with results carried out by ABC Gates Solution must have been stored and available in the ABC Gates Solution for the last year.		
REQ 356.	Transaction logs MUST not contain any personal data, including biometric data.		
REQ 357.	Transaction logs MUST be transferred either continuously or with a delay of no more than 10 minutes to Contracting Authority central log system. A detailed solution for transferring transaction logs will be agreed upon during the contract execution.		
REQ 358.	All transaction logs older than twelve months and that have been transferred to Contracting Authority MUST be deleted.		
REQ 359.	Measures MUST be taken to ensure the integrity of transaction logs when storing and transmitting them.		
REQ 360.	SMIT workstations MUST be used to access and manage ABC Gates Solution.		

REQ 361.	A site-to-site VPN MUST be used to transmit monitoring information.		
REQ 362.	Cryptographic key minimum lengths used in ABC Gates Solution MUST be at least: • AES – 256 bits • RSA – 4096 bits • ECC – 384 bits		
REQ 363.	ABC Gates Service provider MUST be ready to implement post-quantum cryptographic algorithms within 6 months of receiving a request from the Contracting Authority		

12 SERVICE HOSTING REQUIREMENTS

12.1 DATA CENTER AND PLATFORM REQUIREMENTS AND CONSTRAINTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 364.	ABC Solution MUST be implemented as high availability virtualized or container-based solution in two separated SMIT data centers in Estonia.		
REQ 365.	The following platform and infrastructure requirements MUST be observed: Storage: • Object Storage - Scality S3 • File System - Scality NFS • Volume Storage - Nutanix Volumes Virtualization: • Nutanix AHV • KVM Container: • Container Format – OCI • Container Orchestration – Kubernetes • Container Runtime – Docker in VM VM: • Ubuntu • Oracle Linux • Windows Network: • Multilocation loadbalancer - haproxy, VIP		

	• Network topology - data centers have different subnets		
REQ 366.	ABC Gates Service provider MUST describe the resource requirements for the ABC Gates Solution hosting in the procurement tender. The basis for calculation is given in section 2.3 taking account only stages 1-3.		

12.2 NETWORK IMPLEMENTATION REQUIREMENTS AND CONSTRAINTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 367.	The existing SMIT network MUST be used to connect ABC Gates and ABC Management Servers.		
REQ 368.	ABC Gates Service provider MUST describe the network bandwidth and latency requirements between ABC Gates locations and SMIT data centers in the procurement tender. The basis for calculation is given in section 2.3 taking account only stages 1-3.		

12.3 SERVICE AUDITING AND TESTING

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 369.	ABC Gates Service Provider MUST achieve the [ISO/IEC 27001:2022] certification (if the ABC Service Provider does not already have it) not later than the 12 months from launch date of the ABC gate service and MUST maintain it until the end of the contract.		
REQ 370.	Penetration test MUST be completed not later than 6 months from launch date of the ABC Gates service.		

13 REQUIREMENTS TO SERVICE LEVEL AGREEMENT

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 371.	SLA requirements SHALL be applicable per individual ABC gate or ABC Gates management solution.		

REQ 372.	24/7/365 operational schedule model MUST be followed.		
REQ 373.	IT Support Level Tier 1 and Tier 2 MUST be available for 24/7/365		
REQ 374.	Regular maintenance schedule SHALL be agreed in advance with PBGB.		
REQ 375.	Only 1 (one) individual ABC gate SHALL be allowed to close for maintenance at the same time.		
REQ 376.	Maintenance of ABC Gates management and monitoring solution SHALL be agreed with PBGB each time separately.		
REQ 377.	Contingency plans and procedures SHOULD be in place to inform PBGB about these measures.		
REQ 378.	The final requirements for reporting and recording incidents and problems will be agreed upon in the contract.		
REQ 379.	The life cycles of ABC Gates solution hardware components must be defined and their monitoring ensured by the ABC Gates Service provider, submitting them to the Contracting Authority with the offer.		
REQ 380.	Mobile workstations (tablets) MUST be replaced every 3 years with new ones.		
REQ 381.	The replacement of the glass of the ABC Gates document readers MUST execute every 3 years.		

13.1 KEY PERFORMANCE INDICATORS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 382.	Any interruptions and deviations related to the operation, availability and performance of the Contracting Authority's data centers, hardware, software and network MUST be excluded from KPI calculations.		
REQ 383.	Average ABC gate transit time MUST be less than 15s for the following use cases described in P.1 of this document: a. and b.		
REQ 384.	Average ABC gate transit time MUST be less than 10s for the following use cases described in P.1 of this document: d.		
REQ 385.	Average ABC gate transit time MUST be less than 30s for the following use cases described in P.1 of this Document: c.		

REQ 386.	Average ABC gate transit time MUST be less than 25s for the following use cases described in P.1 of this Document: e.		
REQ 387.	IT Support Level Tier 1 response time SHALL be up to 15 minutes.		
REQ 388.	Tier 2 response time via remote access in case of malfunctioning ABC Gates management or monitoring solution SHALL be up to 30 min. in Tallinn Airport or up to 1 (one) hour for other locations.		
REQ 389.	Tier 2 on-site response time SHALL be up to 2 (two) hours.		
REQ 390.	Monthly uptime per 1 individual ABC gate MUST be 99 (ninety-nine) per cent.		
REQ 391.	Monthly uptime for ABC Gates management solution MUST be 99,5 (ninety-nine and half) per cent.		
REQ 392.	Monthly uptime for each connection between ABC Service Provider and Contracting Authority data centers MUST be 99 (ninety-nine) per cent.		
REQ 393.	If one connection between ABC Service Provider and Contracting Authority data centers is lost, traffic MUST automatically be redirected to an alternative route within a maximum of 30 seconds.		
REQ 394.	Maintenance performance window MUST be less than 4 (four) hours.		
REQ 395.	Local document model database MUST be updated at all ABC gates no later than 30 days after the publication of the document model database update by the document reader manufacturer.		
REQ 396.	Number of hardware components that were not replaced during the month were faulty or had reached the end of their life cycle.		

14 STATISTICS AND REPORTING

14.1 SLA REPORTING

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 397.	ABC Gates Service statistics about helpdesk tickets, incidents and problems MUST be provided by ABC Gates Service provider.		

REQ 398.	Statistics ABC Gates Service SLA Key Performance Indicators MUST be provided by ABC Gates Service provider.		
REQ 399.	The PBGB has the right to request changes or additions to the above-named statistics reporting details without additional charge.		
REQ 400.	Statistics reports must be provided once a month, before the 10th of next month.		

15 ADDITIONAL INFORMATION

15.1 EAC AND FINGERPRINT ENROLLMENT

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 401.	The service MUST be delivered with readiness to implement fingerprint 1:1 check using EAC in scenarios described p.1 a. and b.		
REQ 402.	Fingerprint enrollment functionality MUST be added to the ABC gates concurrently with implementation of EES scenarios described in p.1 c. and e.		

15.2 MASTERLIST IMPLEMENTATION

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 403.	The ABC Gates Solution MUST be implemented with integration to Contracting Authority DS Verification Service.		

15.3 LIST OF MESSAGES TO ABC GATES OPERATOR

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 404.	The messages to ABC Gates operators will be agreed with PBGB during execution of the Contract.		

15.4 LIST OF MESSAGES TO A TRAVELLER

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 405.	The messages to traveler will be agreed with PBGB during execution of the Contract.		

16 TRAINING

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 406.	The ABC Gates Service Provider SHALL conduct two types of trainings: a) initial trainings b) refresher trainings.		
REQ 407.	The ABC Gates Service Provider SHALL conduct initial trainings for ABC Gates operators at each ABC Gates installation location in Estonia prior to the initial commissioning and operational use of the ABC Gates solution.		
REQ 408.	Initial trainings related to the ABC Gates base functionality SHALL be conducted as instructor-led on-site training.		
REQ 409.	The Service Provider SHALL provide three (3) initial training sessions at each installation location. The exact training dates shall be agreed with the PBGB.		
REQ 410.	The duration of a single initial training session SHALL NOT exceed eight (8) academic hours.		
REQ 411.	The initial trainings must be conducted for a maximum of 35 people per location.		
REQ 412.	The initial training SHALL be conducted on PBGB premises using the presentation equipment provided by the PBGB.		
REQ 413.	Refresher trainings SHALL be provided at least once every two (2) years and SHALL cover the current ABC Gates functionalities used by the PBGB at the time of the training. Such refresher trainings shall be conducted as instructor-led on-site trainings.		
REQ 414.	The Service Provider SHALL provide three (3) refresher training sessions at each installation location. This applies to every two (2) year period. The exact training dates shall be agreed with the PBGB.		
REQ 415.	The duration of a single refresher training session SHALL NOT exceed eight (8) academic hours.		
REQ 416.	The refresher trainings must be conducted for a maximum of 35 people per location.		

REQ 417.	The refresher trainings SHALL be conducted on PBGB premises using the presentation equipment provided by the PBGB.		
REQ 418.	Both, the initial and refresher trainings SHALL include video-based training materials enabling participants to become familiar with the operation and management of the ABC Gates solution. The trainings SHALL also include practical demonstrations using the gate test mode environment.		
REQ 419.	For both initial and refresher trainings, the Service Provider SHALL develop and provide electronic training materials to the PBGB covering all the current functionalities.		
REQ 420.	The electronic training materials shall be updated by the Service Provider whenever new functionalities or relevant changes are introduced.		
REQ 421.	The electronic training materials SHALL be comprehensive and sufficiently detailed to enable newly appointed ABC Gates operators to independently operate the ABC Gates solution.		
REQ 422.	The Service Provider SHALL provide electronic training materials to the PBGB no later than five (5) working days before any initial training, refresher training, or the go-live of a new functionality. For new functionalities, the obligation to provide training materials applies regardless of whether a dedicated training session is conducted.		
REQ 423.	All training sessions and electronic training materials SHALL be provided in Estonian.		
REQ 424.	The PBGB SHALL have the right to record initial and refresher training sessions for internal operational and training purposes.		
REQ 425.	Training presentations, videos, video recordings and electronic training materials developed, customized, produced or delivered under the Contract shall become the property of the PBGB. The PBGB shall have an unrestricted, perpetual, irrevocable and royalty-free right to use, reproduce, modify, supplement, distribute, publish, share and further develop such materials for operational, educational and training purposes, including within and outside the PBGB. The Service Provider shall ensure that no contractual, intellectual property or licensing restrictions prevent the PBGB from exercising these rights.		
REQ 426.	Both, the initial and refresher trainings SHALL, at a minimum, cover: • overview of the ABC Gates solution architecture and components; • operational principles of the ABC Gates solution;		

	• use of the operator desktop workstation and mobile user interface; • gate monitoring, management and incident handling procedures; • automated document verification processes and checks; • biometric verification processes and result interpretation; • assessment and interpretation of transaction and inspection results; • operator actions in case of failures, alerts, exceptions and suspected fraud cases; • chip security mechanisms and electronic document chip verification procedures, including the interpretation of verification results.		

17 REQUIREMENTS DEFINITION AND TENDER EVALUATION

17.1 REQUIREMENTS DEFINITION

As stated here above in this document all the requirements provided are mandatory if not stated explicitly in another way.

17.2 EXPLANATION OF THE DESCRIPTION OF REQUIREMENTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 1	**[Requirement title]** [Customer's Requirement Description]	*[Vendor to include, or refer to, supporting documentation that prove/support fulfilment of the minimum requirement]*	**Yes/No**
REQ 2	**[Requirement title]** [Customer's Requirement Description]		**Yes/No**

The requirements will be stated as in the example above.

The first column labelled "No." provides a unique number for each requirement, using the prefix "REQ". Requirements are numbered sequentially throughout the document.

The second column labelled "Requirement Description" contains a Requirement Title (bold text) and the Contracting Authority's Requirement Description. The requirements are not scored but evaluated as fulfilled/not fulfilled based on the documentation provided by the Vendor. The Contracting Authority reserves the right to decide if the Vendor fulfils the requirements or not based on the documentation provided.

The third column labelled “Vendor’s Response” shall be filled by the Vendor to include, or refer to, supporting documentation to convince the Customer that the requirement is fulfilled. The referenced documentation should be as short and precise as possible.

In the last column labelled “Fulfilled” the Vendor must clearly state whether the Vendor fulfils the requirement (**Yes**) or not (**No**). Should the column “Fulfilled” not be filled in, then the Customer will assume the column to be filled in with “No” and therefore it will constitute a confirmation that the Vendor cannot comply with the requirements. All other filled values like „partially“, „not available“, etc. are considered as No. as well as leaving the field blank.