For the internal use
Notation made
The access restriction is valid until
Basis: clause 35 (1) 9) and 10) of the Estonia’s Public Information Act
SMIT

REPUBLIC OF ESTONIA
MINISTRY OF THE INTERIOR

Lisa 2 - Tehniline kirjeldus / Technical specification for the Self-service kiosk for Border Control Point

The project is co-financed by the European Union via the Internal Security Fund and Estonian Ministry of Interior ISFB-31 „Creation of Automatic Border Control system (Tallinna-1 ja Narva-1)“

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

Herewith the Contracting Authority has decided to initiate a project to introduce machine readable electronic travel document automated check of the EU citizens subject to a ‘minimum check’ on the Schengen Border in Estonian Republic. The aim of the project is to facilitate MRTD data selfserviced 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 kiosk solution providing more advanced self-services for travellers than is in use at present. The requirements in this Technical Specification are provided to explain the details of technical and procedural parameters to achieve the service level required. The Solution has to be designed in a way which allows for extension in future developments. Foreseeable aspects of future upgrade and extension can be found in Chapter 11 of this Specification.

All the kiosk operations MUST be conformant to the requirement in this Technical Specification and relevant standards in order to guarantee trustworthiness and security of information sent for making border crossing decisions.

The Contracting Authority will install software needed for kiosk operators to the Border Control workstations and tablets.

The Solution is classified as providing Self Service operations according to [BSI-TR-03135-2-v2-1].

The solution is classified as a one-step procedure consisting of following operations:

- Giving directions to the travellers crossing the border;
- Traveller e-MRTD check;
- Facial biometric image capture;
- Comparison of facial images from the facial image capture camera and MRTD DG2;
- Delivery of the comparison result and content of DG1 to the PIKO system of the PBGB;
- Interrupting semi-automatic border crossing procedure and guiding travellers to manual inspection in case of errors in MRTD check or comparison of facial images.

It is recommended to treat the definitions and descriptions as described in "Machine Readable Travel Documents" [ICAO9303] as well as in the ICAO "Technical Report on Machine Assisted Document Security Verification" [ICAOMADSV1]. Regarding modern electronic Identity Documents, the Technical Guidelines [TR-03110], [TR-03121], [TR03127] and [TR-03135] are recommended.

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

All components supplied by the Vendor 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.

Solution component	Scope
Self-service kiosk	The Vendor SHALL set up physically and prepare to connect to CA networks self-service kiosk in border control point to gather and deliver to PBGB PIKO system information needed for making border crossing decisions and operating kiosk according to the instruction commands from the kiosk operator software. The hard- and software upgrade schedule SHALL be agreed with the CA but the Vendor SHALL provide major upgrades to the kiosk and mission and security critical updates upon their becoming available.
Tablets with protective covers and charging docks	Portable devices for observation and control individual kiosk areas locally and from distance.
Kiosk management software user interface version for tablets	Software used for kiosk operating.

Kiosk management software operators' user interface version for desktop workstations	Software used for kiosk operating.
ABC gate management server software solution update	Software update for ABC gate management server software to support the operating of the kiosk according to commands from the kiosk management software.
ABC gate monitoring server software solution update	Software update to support the gathering of technical status information from the kiosk and delivering alerts to the servicing personnel.
Licenses	The Vendor SHALL submit proof that he has all the licenses required to operate the kiosk, contingent hard- and software. Licenses MUST cover all the components purchased in course of this Tender.

Table 1: Scope of Tender

1.2 STRUCTURE OF THIS DOCUMENT

Chapter 2 contains overall requirements. Here description of premises are provided, requirements to the kiosk and components etc. are described.

Chapter 3 contains requirements to system documentation. Documents mandatory to be provided by the Vendor are listed here.

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

Chapter 5 contains technical requirements to the hardware. Physical and operational parameters and details of various hardware components of the Solution are provided here.

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 performing in handling of defective documents.

Chapter 9 contains requirements to data exchange between user interfaces, PIKO and kiosk.

Chapter 10 contains Security aspects of the Solution.

Chapter 11 contains additional information related to readiness to implementation of EAC and also topics due to be agreed during execution of the Contract.

Chapter 12 contains information about the changes in electronic check workflows related to implementation of EAC and changes due to implementation of RCC.

Chapter 13 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 exist 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. One operator or vendor 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.
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.
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.
Kiosk	Self-standing kiosk providing self-service capabilities for border control.
Inspection Application	Software supervising document reading, face enrollment, biometric comparison, data delivery to the PIKO.
Inspection System	In the scope of the present tender the system containing document reading hard- and software, facial image comparison software and user interface to display information to the person at self-service kiosk. 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 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	Term is used to cover all human personnel that require system access to operate, administer or audit the kiosk.
PIKO	Border Control System of the PBGB.
Vendor	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 solution.
ABC Gates Management solution	Secunet Easyserver management and monitoring solution used by Contracting Authority for ABC gates.
Appendix F	FBI interoperability standard for fingerprints. Appendix F has stringent image quality conditions, focusing on the human fingerprint comparison and facilitating large-scale machine many-to-many matching operation.
FAP 50, FAP 60	Fingerprint reader capture area dimension according to the Appendix F
WSQ	A fingerprint image compression algorithm

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	Certification Authority, Chip Authentication, CAN area
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
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
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 ultra violet light
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
VI	Visual (white) light
WSQ	Wavelet Scalar Quantization

Table 4: Abbreviations

1.5 References And Standards

#	Standard	Publisher	Date

[ANSI_X9_62]	ANSI X9.62-2005 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).	ANSI	Nov. 16th, 2005
[BSI_TR_03105_5-1]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03105 version 2.5, Conformity Tests for Official Electronic ID Documents, Part 5.1, version 1.41, Test plan for ICAO compliant Inspection Systems with EACv1		

#	Standard	Publisher	Date
[BSI_TR_03105_5-2]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03105 version 2.5, 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	May 21st, 2010
[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-03121-2]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03121-2 version 4.4, Part 2: Software Architecture	BSI	2018

[BSI TR-03121-3-v1-v4-4]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03121-3 version 4.4, Part 3: Application Profiles and Function Modules Volume 1: Verification ePassport and Identity Card	BSI	2013-2018
[TR-03121 Scheme v4]	Schema and examples for BSI-TR03121, Version 4.4	BSI	2013-2018
[BSI_TR_03127]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03127 version 1.13, Architecture electronic Identity Card and electronic Resident Permit	BSI	March 10th, 2011

#	**Standard**	**Publisher**	**Date**
[BSI TR-03129-v1-1]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03129 version 1.1, “PKIs for Machine Readable Travel Documents” – “Protocols for the Management of Certificates and CRLs”	BSI	2009
[BSI TR-03129-2]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03129-2 ”PKIs for Machine Readable Travel Documents. “Protocols for the Management of Certificates and CRLs – National Protocols for ePassport Application. Version 1.2“	BSI	March 1st, 2016
[BSI TR-03129-P2]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline BSI-TR-03129 “PKIs for Machine Readable Travel Documents. Part 2: Supplemental specifications for public and official authorities. Version 1.3.0“	BSI	2017
[BSI-TR-03135-1-v2-1]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03135 - Machine Authentication of MRTDs for Public Sector Applications Part 1: Overview and Functional Requirements	BSI	2016

[BSI-TR-03135-2-v2-1]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03135 - Machine Authentication of MRTDs for Public Sector Applications Part 2: Application profiles for official document inspection systems	BSI	2016
[BSI-TR-03135-3-v2-3]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03135 - Machine Authentication of MRTDs for Public Sector Applications Part 3: High Level Document Check Interface Specification	BSI	2017
[EN 62368-1:2014]	IEC/EN 62368-1:2014: Audio/video, information and communication technology equipment. Safety requirements.	IEC/EN	
#	**Standard**	**Publisher**	**Date**
[ICAO9303]	Doc 9303 Machine Readable Travel Documents, Seventh Edition, Parts 1 – 12	ICAO	2015
[ICAOMADSV1]	NTWG Technical Report 'Machine Assisted Document Security Verification' Version 1.0	ICAO	July 26th, 2011
[ICAOSACMRTDTR]	ISO/IEC JTC1 SC17 WG3/TF5 Technical Report 'Supplemental Access Control for Machine Readable Travel Documents' Version – 1.1	ICAO	April 15th, 2014
[IEC 62471]	IEC 62471:2006: Photobiological safety of lamps and lamp systems		
[ISO_1831]	ISO 1831: Printing specifications for optical character recognition	ISO	
[ISO10918-1]	ISO/IEC 10918-1: Information technology - Digital compression and coding of continuous-tone still images: Requirements and guidelines		
[ISO 19794-5]	ISO 19794-5: Information Technology – Biometrics – Biometric Data Interchange Formats – Part 5: Face Image Data		

[RFC_4122]	RFC 4122: A UUID URN Namespace	IETF	July 2005
[RFC5246]	The Transport Layer Security (TLS) Protocol Version 1.2	IETF	August 2008
[RFC 5639]	RFC 5639: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation	IETF	March 2010
[TR_LDS_PKI]	Technical Report – LDS and PKI Maintenance Version 1.0.	ICAO	May 5 2011

Table 5: References

2 GENERAL DESCRIPTIONS

2.1 Background Information

Self-service kiosk will be installed in Saatse BCP for both entry and exit as a pilot.

2.1.1 Saatse BCP

On the Figure 1 the plan of the premises in the Saatse BCP is provided. 1-phase 230V 50Hz AC power will be available in Saatse BCP.

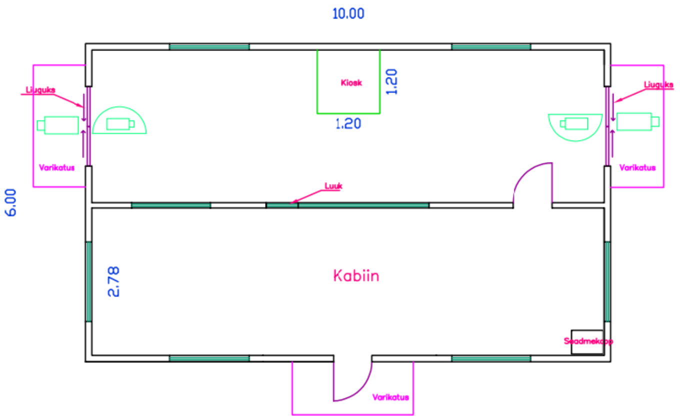


Figure 1. Kiosk location in Saatse BCP

2.2 Safety

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

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 1.	Exiting ABC Gates Management solution SHALL be used for kiosk management and monitoring.		

REQ 2.	There SHALL be connections only to the CA's data network.		

2.3 MANAGEMENT OF MASTERLISTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 3.	Master Lists distribution to Management servers will be accomplished according two scenarios: • Scenario 1 – Local MasterList provided by CA; or • Scenario 2 – DS Verification Service provided by CA • Both scenarios MUST be supported.		

2.4 REQUIREMENTS TO GATE MODULE CONSTRUCTION

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 4.	To be future-proof, an self-service 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.		
REQ 5.	Footprint images MUST be drawn on the floor indicating the standoff distance in front of the camera.		
REQ 6.	Cameras MUST support range of subject heights at standard standoff distance between 1.4 and 2.05 meters.		

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 7.	A kiosk MUST contain of at least: • Facial image capture camera; • Document reader; • Fingerprint reader • Touchscreen display;		
REQ 8.	The kiosk ergonomics, dimensions, location and the environmental conditions SHOULD be considered with a special focus on the needs of travellers with disabilities. NOTE: Handicapped people in wheelchairs or similar will be directed manual border crossing control.		

REQ 9.	A kiosk module MUST have rigid self-standing construction that can be fastened to the floor by means of gluing.		
REQ 10.	All fastenings MUST be covered or special tools MUST be used to operate.		

NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**
REQ 11.	A kiosk MUST meet basic requirements regarding the physical installation and security and safety considerations. This includes protecting the kiosk which is installed in public area 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 12.	The physical parts of the kiosk MUST comply with the applicable fire protection requirements.		
REQ 13.	The kiosk MUST contain lighting module(s) to ensure a proper illumination of the traveller's face area.		
REQ 14.	Graphics with multiple colours or harsh contrasts SHOULD be avoided.		
REQ 15.	Independent switching off of every individual kiosk MUST be supported.		
REQ 16.	Every individual gate MUST have internal independent mains circuit breaker.		

2.5 DOCUMENT READER

NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**
REQ 17.	e-Passport readers SHOULD be positioned at the height of 80-90 cm		
REQ 18.	MRTD MUST be placed on the document reader with the biographical data page facing down and the MRZ side first.		
REQ 19.	Document reader MUST be able to communicate with RFID chips in both locations – either in MRTD data page or back cover.		

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 20.	Document reader MUST be full-page type. Swipe-type document reader MUST NOT be used.		
REQ 21.	Document Reader MUST be supplied together with document model catalogue in machine readable form according to the defined XML schema of [BSI-TR-031351-v2-1] which summarizes all necessary information on the spectrally selective verification checks.		

Figure 8: Graphic instruction how to place the e-Passport on the reader

2.6 FACIAL IMAGE CAPTURE CAMERA

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 22.	There MUST be one facial image capture camera per one KIOSK.		
REQ 23.	The default height setting of the self-adjusting camera MUST be configurable.		
REQ 24.	Facial image capture camera MUST have optical autofocus.		

2.7 FINGERPRINT READER

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 25.	There MUST be one fingerprint reader per one kiosk.		

2.8 USER INTREFACES (SCREENS)

2.8.1 TRAVELLERS' SCREEN INTERFACE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 26.	Screen(s) MUST be large enough to be observed by the travellers to use the kiosk.		

REQ 27.	The screen(s) must offer guidance and live video feedback to the traveller (digital mirror).		
REQ 28.	Screen(s) position MUST be selected based on ergonomics and convenience to the travellers.		

2.8.2 KIOSK OPERATOR'S DESKTOP WORKSTATION INTERFACE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 29.	Part of the workstation screen MUST be reserved for 1 or 2 images of Milestone security surveillance solution camera feed supplied by the PBGB and not integrated with the kiosk monitoring application. No. of camera feeds will depend on system configuration of the BCP.		
REQ 30.	Details of the kiosk operator's desktop workstation user interface SHALL be agreed with the CA during the execution of the Contract.		

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 31.	Upper part of the screen (Kiosk monitoring area) MUST show at the same time: • Kiosk status for up to the 4 kiosks; and • Alerts from the PIKO system.		
REQ 32.	Lower part of the tablet screen MUST be reserved for 1 or 2 images of Milestone security surveillance solution camera feed supplied by the PBGB and not integrated with the kiosk monitoring application. No. of camera feeds will depend on system configuration of the BCP.		
REQ 33.	Details of the kiosk operator's mobile user interface SHALL be agreed with the CA during execution of the Contract.		

2.9 KIOSK IDENTIFICATION

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 34.	Each kiosk SHOULD be uniquely identified.		
REQ 35.	The Vendor MUST accept possibility that numbering syntax and interval will be prescribed by the CA.		

2.10 Kiosk operating conditions

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 36.	The Kiosk MUST be operative at ambient temperatures 5 – 35 degrees Centigrade.		
REQ 37.	The Kiosk MUST be operative at ambient humidity 30 – 70 per cent.		

2.11 Requirements to kiosk functionality

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 38.	The kiosk MUST have IS client functionality for CSCA (and CVCA) PKI operations.		

3 REQUIREMENTS TO SYSTEM DOCUMENTATION

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 39.	The Vendor SHALL, for all software and equipment (hardware) offered, provide general system documentation written in English covering the following items: • Kiosk operator desktop workstation and mobile UI operating manuals.		

4 REQUIREMENTS TO THE KIOSK MANAGEMENT

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 40.	The kiosk management MUST have GUI solution for desktop computers.		
REQ 41.	The kiosk management MUST have GUI solution for tablets.		
REQ 42.	Personal data acquired during passenger check MUST NOT be stored in the management and monitoring system.		
REQ 43.	Manual override by the kiosk operator of the status (operational/non-operational) of an individual kiosk MUST be supported.		

5 TECHNICAL REQUIREMENTS TO THE HARDWARE

5.1 DOCUMENT READER

5.1.1 DOCUMENT FORMATS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 44.	Document reader MUST support TD1 format of MRTDs specified in [ICAO9303]		
REQ 45.	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 46.	Document data page SHALL be optically recorded and digitized under IR, VI and UV spectral range light.		
REQ 47.	The optical resolution SHALL be at least 385 ppi.		
REQ 48.	Reading of MRZ and CAN MUST be supported.		
REQ 49.	Document reader sensitivity to incoming ambient light MUST be minimized by: shielding by technical safeguarding measurements; by compensating of external light; or by both methods.		
REQ 50.	OCR of data both in MRZ and CAN MUST be supported.		
REQ 51.	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 restrict passage and redirect the traveller to travel document 2nd level of inspection.		
REQ 52.	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 53.	Reading of chips compliant to ISO 14443 Type A and B, ICAO LDS 1.7, PKI 1.1 MUST be supported.		
REQ 54.	Transmission protocol T=CL MUST be supported.		

REQ 55.	Data exchange rates 106, 212, 424 and 848 kbps MUST be supported.		
REQ 56.	Chip detection in any part of the document MUST be supported.		
REQ 57.	Chip MUST be readable when document is positioned on the optical reading surface.		
REQ 58.	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 59.	Document reader MUST have the following certifications - CE, RoHS, EN 62368-1, EN62471.		
REQ 60.	Document reader MUST have the following certifications - [BSI_TR_03105_5-1] and [BSI_TR_03105_5-2]		
REQ 61.	The RF-reading module of the document reader MUST be certified according to [TR-03105-4]		
REQ 62.	The document reader MUST comply with the existing regulations regarding EMC and UV-A light emission.		

5.1.5 Performance capabilities and temporal requirements

No.	Requirement Description	**Vendor's Response**	**Fulfilled**
REQ 63.	On the average, optical images of the MRZ MUST be captured within 2 seconds		
REQ 64.	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 65.	Document verification MUST start as soon as the input data becomes available to the system.		
REQ 66.	Full document verification process of an electronic MRTD[3] SHALL NOT take longer than 7 seconds[4].		

[1] Corresponds to t_1 on the Figure.

[2] Estonian passport of 2021 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 3.

5.1.6 COMMUNICATION REQUIREMENTS FOR THE RF-READING MODULE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 67.	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 [ISO14443]		

5.1.7 CHIP APPLICATION SUPPORT

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 68.	Applications to be supported: • e-Passport (DG01 – DG16); and • e-ID (DG01 – DG21)		

5.1.8 AUTOMATION REQUIREMENTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 69.	Automatic detection of document placing MUST be supported.		
REQ 70.	Document scanning process MUST start automatically		
REQ 71.	Technical solutions enhancing reading quality of the MRTDs are RECOMMENDED.		

5.2 FINGERPRINT READER

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 72.	Minimal frame rate for slaps > 5 fps is REQUIRED.		
REQ 73.	4-4-2 flat fingerprint enrollment MUST supported.		
REQ 74.	Fingerprint reader MUST NOT use total internal reflection technology.		

5.3 IMAGE CAPTURE CAMERA

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED

REQ 75.	The minimum physical resolution of the camera video stream MUST be at least 12 megapixels.		
REQ 76.	The camera system SHALL adapt automatically to the height of the person standing in front of it.		
REQ 77.	The camera system SHALL cover at least a range of 140cm to 205 cm of a person's body height (if standing in marked position in front of the camera system).		
REQ 78.	The camera SHALL be able to capture a frontal image of the person if the person is looking straight to the image capture camera.		
REQ 79.	The camera system SHALL guarantee sharpness of the captured facial image if the traveller is positioned within the designated capture area.		
REQ 80.	The camera system SHALL minimise distortion of the captured facial image within the whole capture area.		
REQ 81.	The camera system SHALL provide live stream for traveller instruction screen and guidance for the traveller.		
REQ 82.	If the person is looking straight to the traveller instruction screen the viewing direction of the person SHALL be frontal.		
REQ 83.	The facial images provided by the capture unit MUST have at least 120 pixels between the centers of the eyes.		

5.3 LIGHTING

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 84.	Active diffuse lighting SHALL be used to ensure uniform illumination of the captured facial image and to be independent of external lighting.		
REQ 85.	The lighting SHALL NOT cause reflections on glasses or the skin of the face.		
REQ 86.	The lighting MAY be active during the complete capture process and brightness MAY be varied to get best contrast and illumination.		

5.4 TABLET

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 87.	The screen size MUST be ≥10 to <13”.		
REQ 88.	The screen ratio of the tablet MUST be 9 to 16.		

REQ 89.	The screen MUST be touch sensitive.		
REQ 90.	The screen brightness MUST be at least 300 cd per sq. m.		
REQ 91.	Battery runtime MUST be at least 8 hours.		
REQ 92.	The tablet orientation in dock during charging MUST be portrait.		
REQ 93.	The tablet MUST have NFC connectivity.		
REQ 94.	The tablet MUST have 4G and WiFi connectivity.		
REQ 95.	The tablets MUST have Windows 10 Pro operating system.		
REQ 96.	The tablets MUST support at least WPA2 WiFi encryption.		

6 REQUIREMENTS TO THE PROCEDURES OF DOCUMENT READING AND VERIFICATION PROCESS

Chapter 6 describes data processing procedures that MUST be performed during a 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 97.	Unique monotonously increasing identification number MUST be attributed to every individual document check transaction.		
REQ 98.	Other principle than provided in RFC 4122 MAY be used for document check transaction numbering.		
REQ 99.	All travellers whose document check aggregate result will not be 'successful' MUST be redirected to manual document check. Corresponding guidance SHALL be displayed on the traveller's screen interface		
REQ 100.	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 6.

Result of the check	**Traffic light color**

Successful	green
Failed	red
Undetermined	yellow
Not supported	grey
Aborted	black

Table 6.

6.2 WORKFLOW

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 101.	Data in VIZ SHALL NOT be used for document optical checks.		
REQ 102.	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 103.	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 104.	Optical checks MUST be performed.		
REQ 105.	Electronic checks MRZ MUST be performed.		
REQ 106.	Biometric checks MUST be performed.		

REQ 107.	Combined checks MUST be performed.		
REQ 108.	Requests into background systems MUST be performed.		

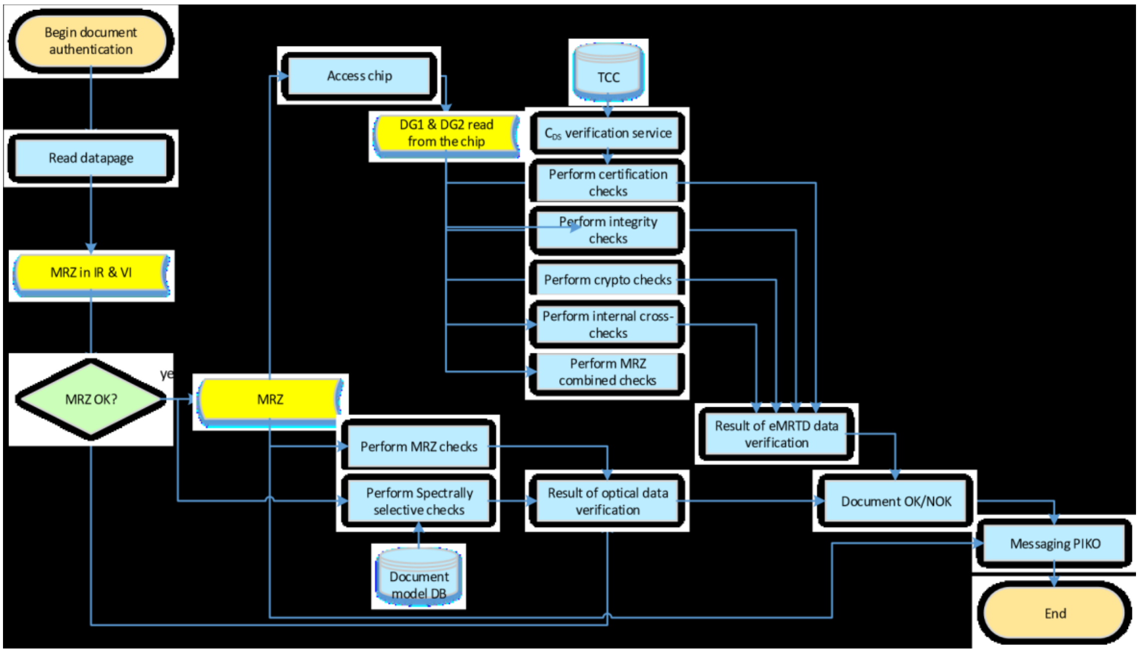

Begin document authentication
Read datapage
MRZ in IR & VI
MRZ OK?
ye
MRZ
Access chip
DG1 & DG2 read from the chip
TCC
C$_{DS}$ verification service
Perform certification checks
Perform integrity checks
Perform crypto checks
Perform internal cross-checks
Perform MRZ combined checks
Result of eMRTD data verification
Perform MRZ checks
Perform Spectrally selective checks
Document model DB
Result of optical data verification
Document OK/NOK
Messaging PIKO
End

Figure 3. Process sequence of checking MRTDs

6.4 Process Sequence of Checking a MRTD

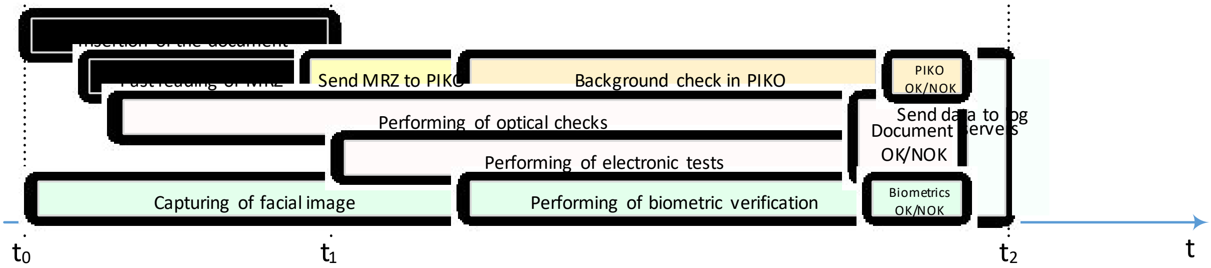


Figure 3. Temporal sequence of MRTD checking process

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 during 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.

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 109.	Compatibility to the schema on Figure 3 MUST be followed.		
REQ 110.	Fast MRZ functionality MUST be supported.		
REQ 111.	Fast MRZ functionality MUST enable to finish reading MRZ within 1 second after travel document reaching its final reading position.		

6.5 Optical checks

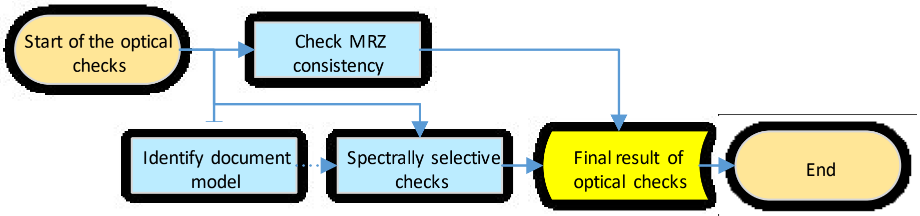

Start of the optical checks
Check MRZ consistency
Identify document model
Spectrally selective checks
Final result of optical checks
End

Figure 4. Principal process sequence of optical checks.

6.5.1 Document model

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 112.	Manufacturer- and model-specific check routines SHALL be classified and logged according to the schema given in [BSI-TR-03135-1-v2-1] table 4.2.		
REQ 113.	The result of the document model identification SHALL be mapped regarding the following list: • The result of the document model identification MUST be set to 'successful' if the model was determined and a selection was made; • The result of the document model identification MUST be set to 'undetermined' if the model could not be determined and a selection was not made; • The result of the document model identification MUST be set to 'aborted' if checking process was aborted prior to its defined process flow. A handling, software, or other type of error occurred.		

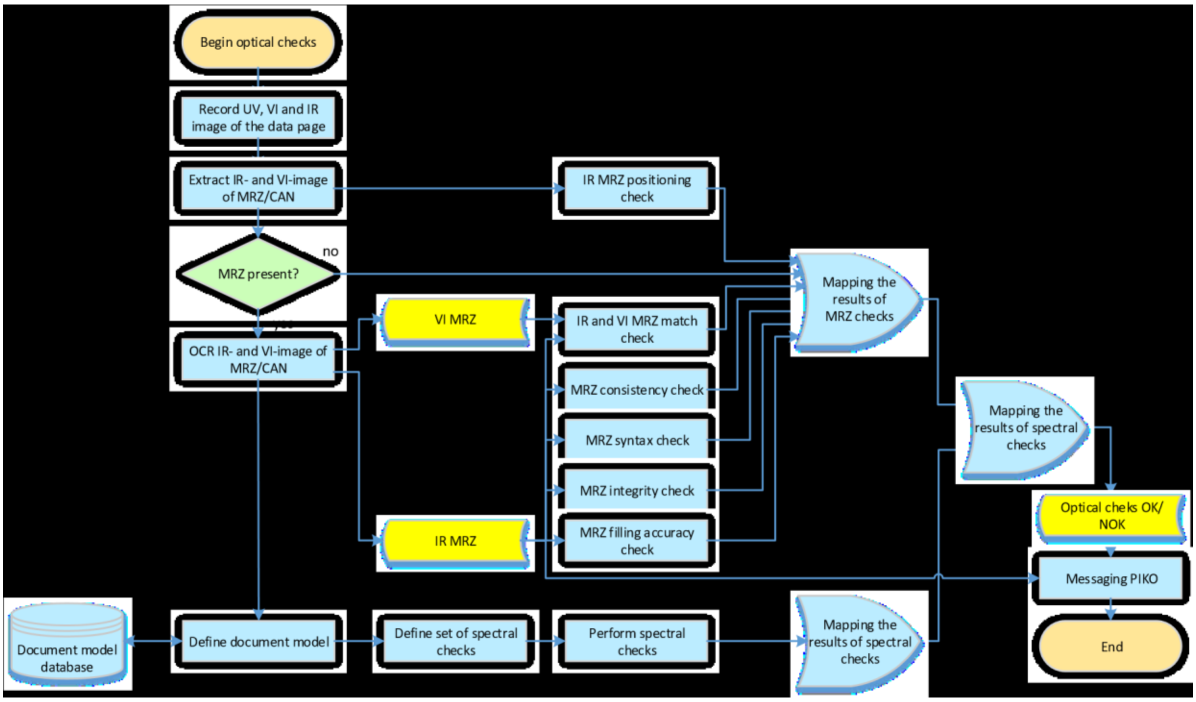

Begin optical checks
Record UV, VI and IR image of the data page
Extract IR- and VI-image of MRZ/CAN
IR MRZ positioning check
MRZ present?
no
Mapping the results of MRZ checks
VI MRZ
IR and VI MRZ match check
OCR IR- and VI-image of MRZ/CAN
MRZ consistency check
MRZ syntax check
Mapping the results of spectral checks
MRZ integrity check
Optical cheks OK/ NOK
IR MRZ
MRZ filling accuracy check
Messaging PIKO
Document model database
Define document model
Define set of spectral checks
Perform spectral checks
Mapping the results of spectral checks
End

Figure 5. Detailed process sequence of optical checks

6.5.2 Requirements to the optical check procedures

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 114.	Optical checks must be performed according to [BSI-TR03135-1-v2-1] pp. 4.4.3.1 and 4.4.3.2.		
REQ 115.	MRZ contents MUST be read in IR light.		
REQ 116.	MRZ contents MUST be read in VI light.		
REQ 117.	CAN contents MUST be read in IR light.		
REQ 118.	CAN contents MUST be read in VI light.		
REQ 119.	Optical quality (i.e. printing clearness etc.) of the MRZ MUST be checked.		
REQ 120.	MRZ (CAN) contents SHALL be OCRed.		
REQ 121.	Positioning of the MRZ according to [ICAODOC] Part 4 p.3 Figure 3 in bounding rectangle limits MUST be verified.		
REQ 122.	Consistency of MRZ MUST be checked.		
REQ 123.	Syntax of MRZ MUST be checked.		
REQ 124.	Integrity of MRZ MUST be checked.		
REQ 125.	MRZ consistency, syntax and integrity checks MUST be performed on basis of the result of IR OCR.		

REQ 126.	Accuracy of MRZ filling-in MUST be verified.		
NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**
REQ 127.	Set of spectrally selective checks MUST be compiled on the basis of document model database.		
REQ 128.	At least following spectrally selective checks MUST be performed: • presence of UV fibres; • data page UV dullness; • presence of MRZ overprint in VI, IR; • Static printed feature in IR.		
REQ 129.	The results of optical checks MUST be mapped regarding the following list: • The result of the check MUST be set to 'successful' if all check routines gave correct results. • The result of the check MUST be set to 'failed' if at least one check routine has incorrect result. • Otherwise the check MUST be set to 'undetermined'. • The check MUST be set to 'aborted' if due to an error the checking process was aborted prior to its defined process flow.		

6.6 ELECTRONIC CHECKS OF MRTDS

6.6.1 SUPPORT OF THE FOLLOWING ALGORITHMS, PROTOCOLS AND SECURITY MECHANISMS

NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**
REQ 130.	DH and ECDH key agreement algorithms MUST be supported.		
REQ 131.	BAC according to [ICAO9303] Part 11 MUST be supported.		
REQ 132.	PACE according to [ICAO9303] Part 11 MUST be supported.		
REQ 133.	PA according to [ICAO9303] Part 11 MUST be supported.		
REQ 134.	AA according to [ICAO9303] Part 11 MUST be supported.		
REQ 135.	Terminal Authentication (TA v1, TA v2) MUST be supported.		
REQ 136.	Chip Authentication (CA v1, CA v2) MUST be supported.		

6.6.2 Files and data groups to be supported

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 137.	EF.COM		
No.	Requirement Description	Vendor's Response	Fulfilled
REQ 138.	EF.SOD V1		
REQ 139.	EF.SOD V2		
REQ 140.	DG14		
REQ 141.	DG15		
REQ 142.	EE.CVCA		
REQ 143.	EF.CardAccess		
REQ 144.	EF.CardSecurity		
REQ 145.	EF.ChipSecurity		
REQ 146.	DG1		
REQ 147.	DG2		
REQ 148.	DG3		

6.6.3 Electronic check flowcharts

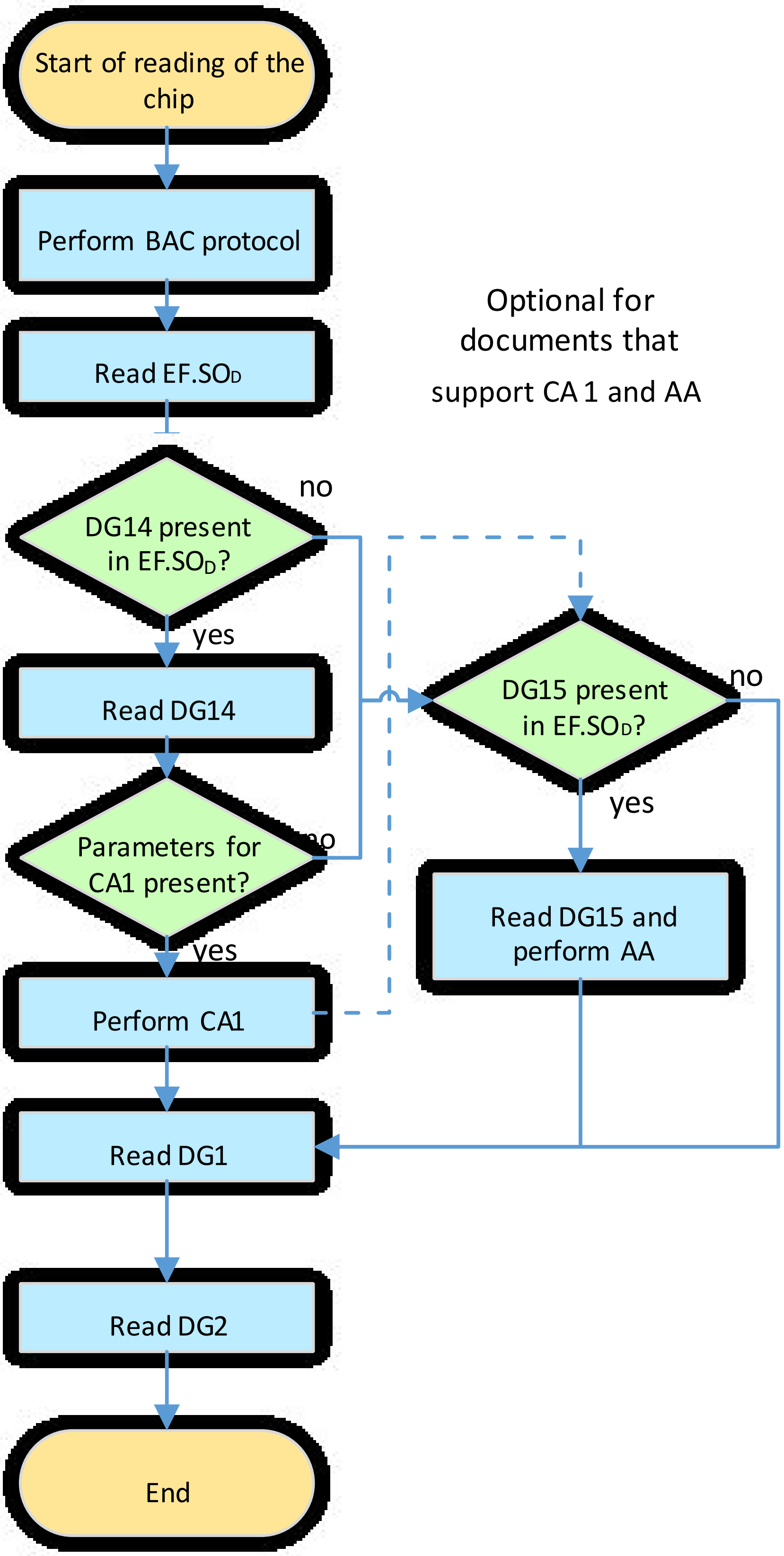


Figure 6. Protocol Sequence 1 performing BAC

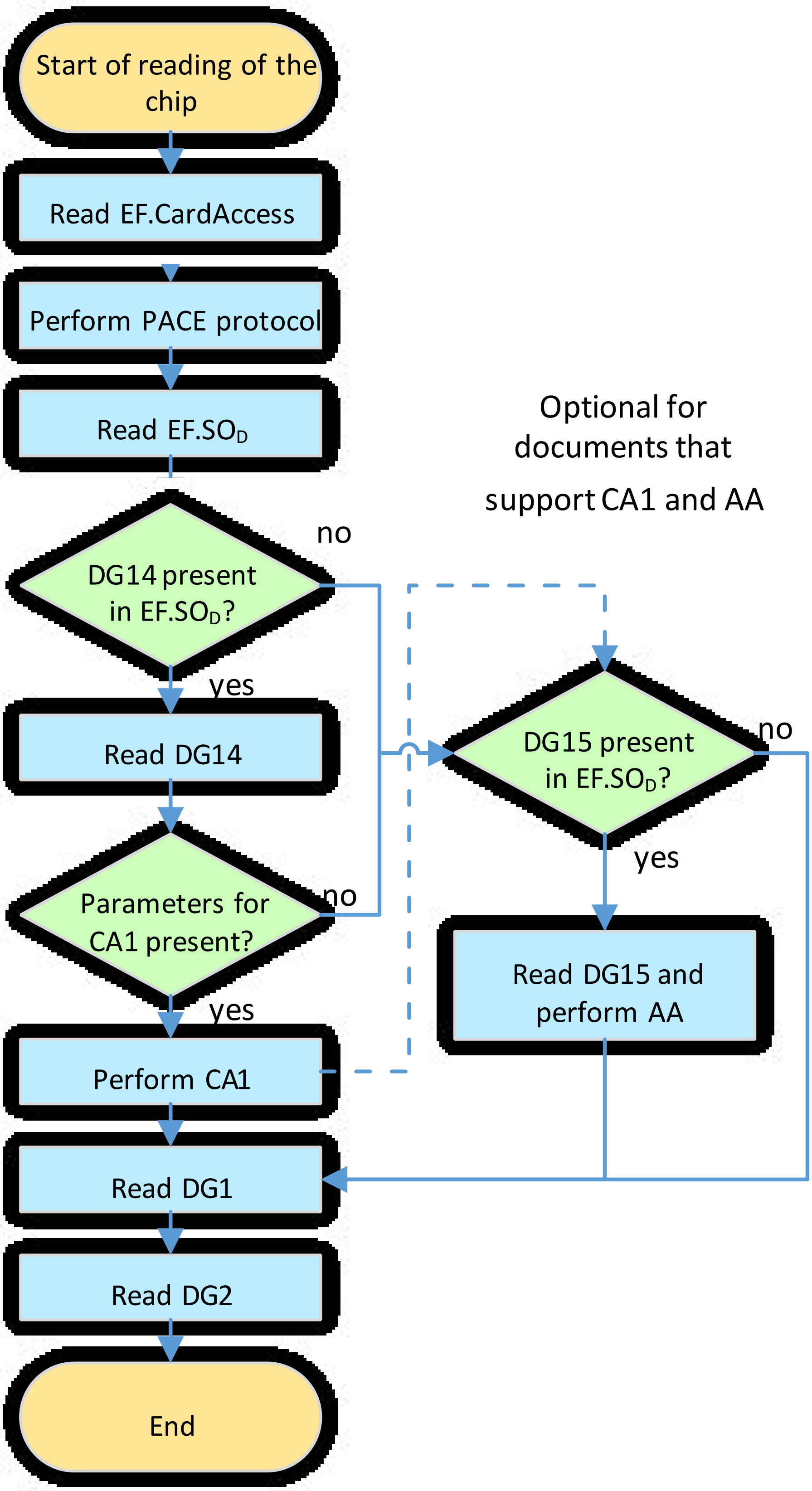

Start of reading of the chip
Read EF.CardAccess
Perform PACE protocol
Read EF.SO$_D$
Optional for documents that support CA1 and AA
DG14 present in EF.SO$_D$?
no
yes
Read DG14
Parameters for CA1 present?
no
yes
Perform CA1
DG15 present in EF.SO$_D$?
no
yes
Read DG15 and perform AA
Read DG1
Read DG2
End

Figure 7. Protocol Sequence 2 performing PACE, CA1 or AA

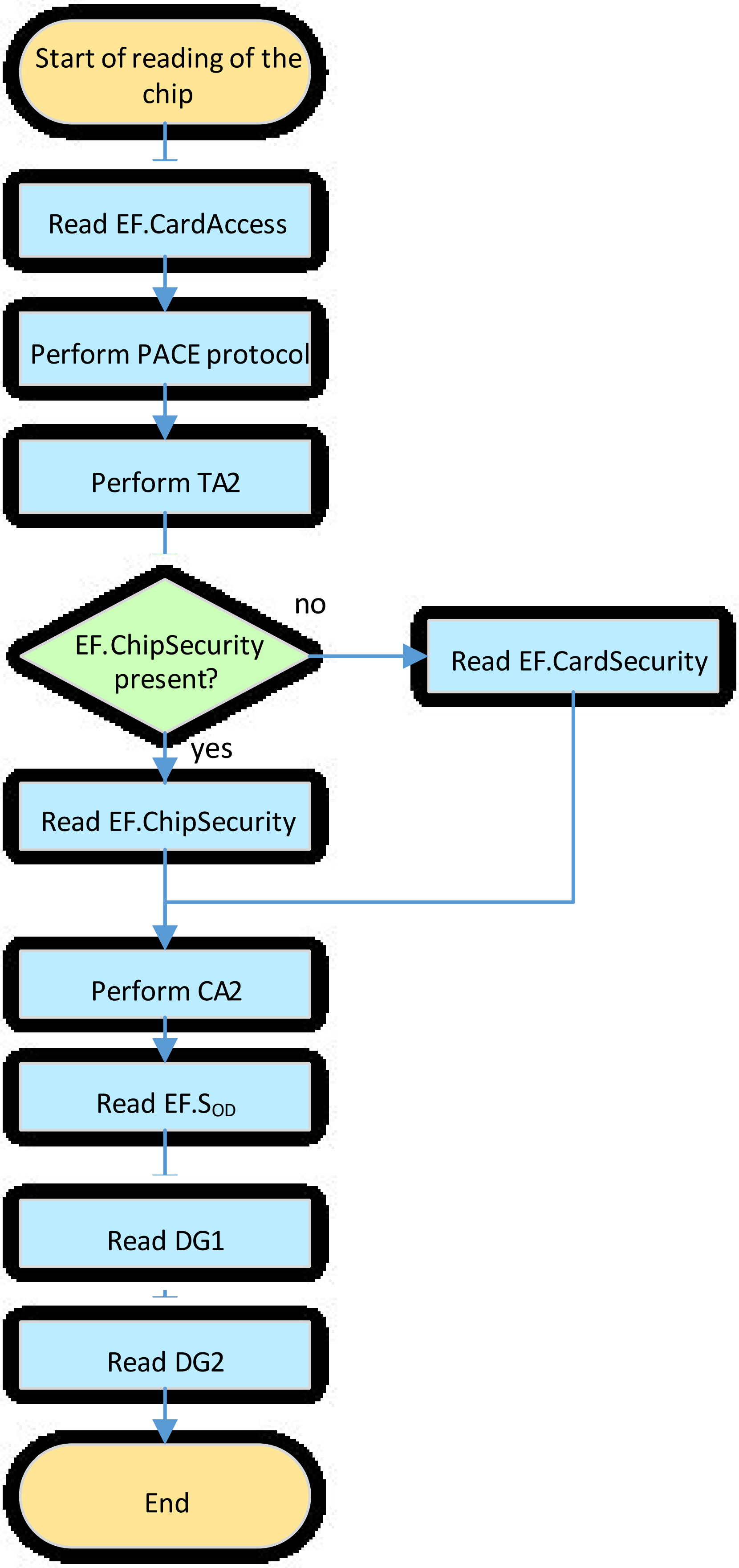


Figure 8. Protocol Sequence 3, performing PACE, TA2, CA2

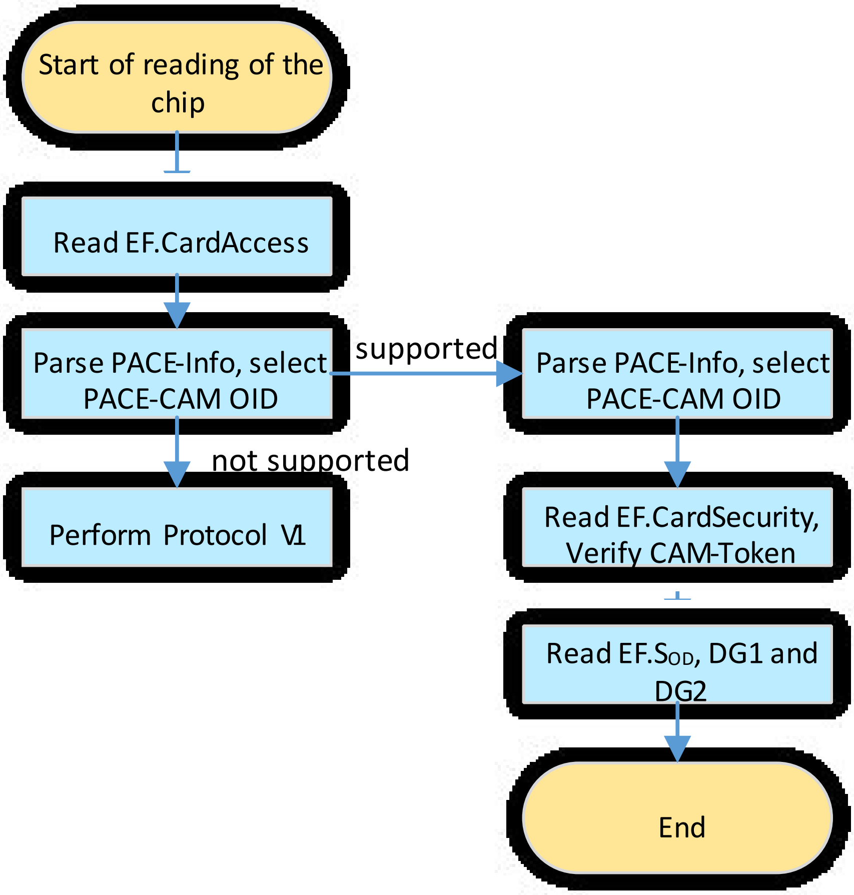

Start of reading of the chip
Read EF.CardAccess
Parse PACE-Info, select PACE-CAM OID
supported
not supported
Perform Protocol V1
Parse PACE-Info, select PACE-CAM OID
Read EF.CardSecurity, Verify CAM-Token
Read EF.S$_{OD}$, DG1 and DG2
End

Figure 9: Protocol Sequence 4, support of PACE-CAM

6.6.4 Processing sequences

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 149.	Process sequence shown in figure 3 MUST be supported.		
REQ 150.	Process sequence shown in figure 4 MUST be supported.		
REQ 151.	Process sequence shown in figure 5 MUST be supported.		
REQ 152.	Process sequence shown in figure 6 MUST be supported.		
REQ 153.	Process sequence shown in figure 7 MUST be supported.		
REQ 154.	Process sequence shown in figure 8 MUST be supported.		
REQ 155.	Process sequence shown in figure 9 MUST be supported.		

6.6.5 Chip access using BAC or PACE protocols

No.	Requirement Description	Vendor's Response	Fulfilled

REQ 156.	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 157.	The inspection system SHALL not use both – BAC and PACE in the same session if fallback is not required.		
REQ 158.	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.		

6.6.5.1 Chip access via BAC

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 159.	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.		

6.6.5.2 Chip access via PACE

No.	Requirement Description	Vendor's Response	Fulfilled

REQ 160.	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.		

6.6.6 Checking Chip Access by Terminal Authentication (TA)[4]

No.	**Requirement Description**	**Vendor's Response**	**Fulfilled**
REQ 161.	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.		

6.6.7 Checking the chip authenticity (AA, CA)

No.	**Requirement Description**	**Vendor's Response**	**Fulfilled**
REQ 162.	The system MUST support altering the chip authenticity checking algorithm sequence.		
REQ 163.	CA is RECOMMENDED to be used if both protocols (CA and AA) are supported by the document chip.		

REQ 164.	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 165.	If only one of the checks from pp. 7.6.7.1 and 7.6.7.2 is 'not supported' and the other one is 'successful' or 'failed' the final result is 'successful' or 'failed'. If both results are 'not supported' the final result is also 'not supported' and the traveller MUST be redirected to manual inspection.		

6.6.7.1 CHECKING CHIP AUTHENTICITY WITH AA

NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**
REQ 166.	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.		

6.6.7.2 Checking chip authenticity with CA

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 167.	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.		

6.6.8 Checking the electronic data authenticity with Passive Authentication (PA)

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 168.	C_{DS} authenticity may be confirmed only either by local ML deliverable by the CA or via TCC PA service.		

6.6.9 MasterList implementation

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 169.	The kiosk SHALL be delivered with DS Verification Service readiness.		

6.6.10 Verification of the security objects

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 170.	Ability to process security objects with one, several or no C_{DS} MUST be supported.		
REQ 171.	Verification of the hash and signature for EF.CardSecurity and mapping to its own final check result (if existing) MUST be performed.		

REQ 172.	Verification of the hash and signature for EF.ChipSecurity and mapping to its own final check result (if existing) MUST be performed.		
REQ 173.	Verification of the hash and signature for EF.SO$_D$ and mapping to its own final check result MUST be performed.		
REQ 174.	Verification of the digital signature of a security object MUST be performed.		
REQ 175.	Comparison of the stored and calculated on site security object's hash values MUST be performed.		
REQ 176.	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 ensure that each DG listed in EF.SO$_D$ is also contained in EF.COM and vice versa.		
REQ 177.	The result of checking of 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.		

6.6.11 Checking issuer certificates

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 178.	Check of the issuer certificate for EF.SO$_D$ MUST be performed.		
REQ 179.	Check of the issuer certificate for EF.CardSecurity MUST be performed.		
REQ 180.	Check of the issuer certificate for EF.ChipSecurity MUST be performed.		
REQ 181.	Check of C_{DS} signature against its respective C_{CSCA} MUST be performed.		

REQ 182.	Check if the document inspection time is within the validity period of the C_{DS} MUST be performed.		
REQ 183.	Check of the revocation state of the C_{DS} MUST be performed.		
REQ 184.	Trust Status MUST be assessed to the Certificates.		

NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**
REQ 185.	The cumulative result of checking of the issuer certificates MUST be mapped regarding the following list[5]: • 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 186.	In case the cumulative result of checking of the issuer certificates is not set to 'successful' the traveller SHALL be redirected to manual inspection.		

6.6.12 CHECKING INTEGRITY OF CHIP CONTENTS

NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**
REQ 187.	Check whether each data group listed in EF.SO_D is also included in EF.COM MUST be performed.		
REQ 188.	Integrity check of all data groups MUST be performed.		
REQ 189.	Integrity check of each individual data group MUST be performed.		

NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**

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

REQ 190.	The result of checking of the integrity of chip contents 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.		

6.6.12.1 Comparing EF.SOD with EF.COM

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 191.	Check whether each data group listed in EF.SOD is also included in EF.COM MUST be performed.		
REQ 192.	The result of comparing EF.SOD 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.SOD are consistent with each other. • Failed – The result of the check must be set to 'failed' if inconsistencies between EF.COM and EF.SOD were detected. • Not supported – The result of the check must be set to 'not supported' if comparing the contents of EF.SOD and EF.COM is not possible, e. g. because one or both files are not on the document. • Aborted – The result of comparing EF.SOD with EF.COM MUST be set to 'aborted' if comparing EF.SOD and EF.COM was aborted due to an error.		

6.6.12.2 Checking data group integrity

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 193.	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.SOD.		

No.	Requirement Description	Vendor's Response	Fulfilled

REQ 194.	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 final 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.SOD with EF.COM MUST be set to 'aborted' if building the final result or an underlying, specific check was aborted.		

6.6.13 Comparison of the issuing state (DG1 and DS certifcate)

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 195.	Comparison of the issuing country (country codes in DG1 and C_{DS}) MUST be performed.		
REQ 196.	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.SOD with EF.COM MUST be set to 'aborted' if comparison of the issuing states was aborted.		

6.7 Combined checks

6.7.1 Cross verification of MRZ data

No.	Requirement Description	Vendor's Response	Fulfilled

REQ 197.	Cross-verification of data retrieved from MRZ and DG1 of the RFID chip MUST be performed.		
REQ 198.	Cross-verification of MRZ data SHALL be performed comparing OCR results of (IR, AB, MR), (VI, AB, MR) and DG1.		
REQ 199.	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.		

6.7.2 VERIFICATION OF DOCUMENT VALIDITY

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 200.	Verification of MRTD validity based on retrieved information from MRZ MUST be performed.		
REQ 201.	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.		

6.8 BIOMETRIC ENROLLMENT AND CHECKS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 202.	Kiosk must be configurable for using non-EES mode or EES mode		

REQ 203.	Reference image SHALL be acquired from the DG2 of the travel document.		
REQ 204.	Comparison of holder's facial image in the eMRTD DG2 to the live image collected from the image capture camera MUST be performed.		
REQ 205.	PAD detection MUST be supported by the camera and fingerprint reader solution. The kiosk 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.		

6.8.1 REQUIREMENTS TO THE CAMERA IMAGE QUALITY

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 206.	All face images captured by camera MUST be compliant with COMMISSION IMPLEMENTING DECISION (EU) 2019/329		
REQ 207.	Captured and framed image size must be 1600x1200 px.		
REQ 208.	Colour depth of facial image processed MUST be 24-bit RGB.		
REQ 209.	Minimal camera resolution MUST be at least 12 MPx		
REQ 210.	The face SHALL be fully visible in the foreground of the provided image.		
REQ 211.	The minimum distance between both eyes for capture positions of the passenger in the preferred area of the camera range SHALL be corresponding to EES requirements.		

6.8.2 REQUIREMENTS TO THE CAMERA IMAGE QUALITY ASSURANCE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 212.	Pre-qualification of captured live facial images from the acquisition stream MUST be used.		
REQ 213.	Capturing of images other than live facial – for example on the shirt – MUST be avoided.		
REQ 214.	Ranking of images according to the conducted prequalification SHALL be used.		
REQ 215.	Images SHALL be passed to the verification stage as indicated by the rank.		

REQ 2016.	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.		
REQ 217.	Quality assessment algorithm used for face images must be same as eu-Lisa proposed or mapping to eu-Lisa algorithm thresholds must be used.		
REQ 218.	Face image quality threshold must be configurable.		

6.8.1 REQUIREMENTS TO THE FINGERPRINT IMAGES QUALITY

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 219.	All fingerprint images MUST be compliant with COMMISSION IMPLEMENTING DECISION (EU) 2019/329		
REQ 220.	WSQ image format MUST supported.		
REQ 221.	Resolution 500ppi is REQUIRED.		
REQ 222.	256 levels of grayscale dynamic range is REQUIRED.		

6.8.2 REQUIREMENTS TO THE FINGERPRINTS IMAGE QUALITY ASSURANCE

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 223.	NFIQ 2.0 quality assessment algorithm used for fingerprint images		
REQ 224.	Quality threshold MUST be configurable.		

6.8.3 REQUIREMENTS TO THE LOCAL BIOMETRIC COMPARISON AT KIOSK

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 225.	The face extraction algorithm security level (threshold) to obtain different values of FTA and FTE MUST be configurable.		
REQ 226.	The vendor of the verification algorithm MUST provide calibration data based on the actual verification performance.		
REQ 227.	The output of the algorithm SHALL be a comparison score[6] 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 228.	The Vendor SHALL provide a DET curve of the algorithm performance.		
REQ 229.	Such performance SHALL be on the basis of images of comparable characteristic (e.g. images in size and resolution and pose variation of a typical ePassport deployment).		
REQ 230.	The FRR shall be less than 4% at a FAR of 0.1%.		

6.8.4 REQUIREMENTS TO THE LOCAL BIOMETRIC COMPARISON CODING AT KIOSK

This sub-clause describes requirements for the coding used during the verification process of facial images.

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 231.	All results of the verification work flow SHALL be encoded in XML as "ph-vid-verify"[7].		

6.9 ERROR CODES AND LOGGING

6.9.1 TRANSACTION LOGGING

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

[7] The XML encoding is defined by the XML schema definition in [TR-03121 Scheme v4] 'vid4v3.xsd'. Examples can be found in 'phvid-verify.xml'.

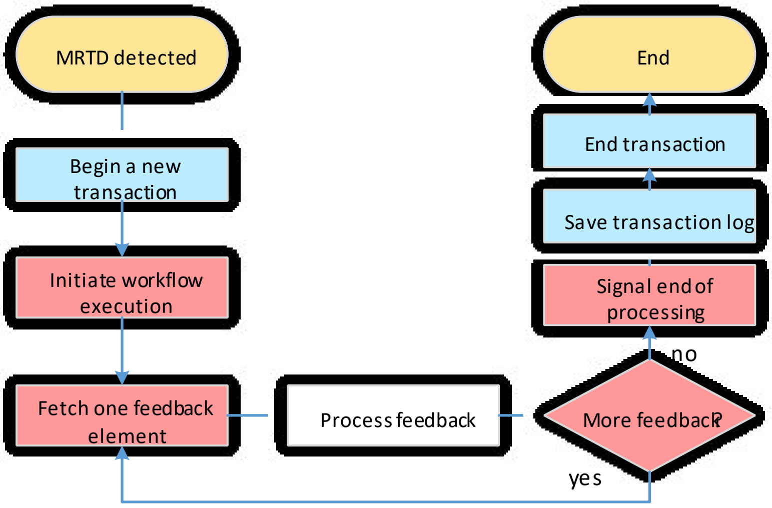


Figure 10: Workflow-based document check with TR-03135-1-compliant logging

Figure 11 shows the extension of the client side of the document check process with transaction logging operations (highlighted in blue). The client initiates a new transaction after a MRTD was detected and before initiating workflow execution. After the workflow execution and result processing is finished, the client requests saving of the corresponding transaction log and then ends the transaction. [BSI-TR-03135-3-v2-3] Section 4.2 provides a quick overview of the interface functions.

Logging is done for the purpose of having continuous quality control, the extraction of business statistics and improvement of the ABC gate system.

Purpose of this requirement is to preserve information that can be given to document issuing authorities to help to solve regular problems with one or another production batch of the travel documents issued by them. It is not very rare, when some production or personalised sets of MRTDs have repeating problems during inspection in another country/countries and therefore it is nearly impossible to trace the problem.

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 232.	No personal, document or border crossing procedure information is stored or logged in the kiosk. 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 233.	The following global states of an inspection process will be logged: • Successful • Terminated • Aborted		

REQ 234.	The result of an inspection process will be logged: • Successful • Failed • Undetermined • Not supported • Aborted		
REQ 235.	Processing errors of each of the checks prescribed in this Technical Specification resulting in an aborted check MUST be logged together with timestamp and kiosk unique identifier.		
REQ 236.	System error codes together with timestamp and unique kiosk 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 237.	Error code message syntax MAY be specified by the Vendor, will be agreed with the Contracting Authority and SHALL contain at least following items: • error code; • kiosk unique identifier; and • timestamp.		

NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**
REQ 238.	Each error code MUST be in unique numeric integer format number. Return code consists of a 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 239.	Logging of all relevant check results which is provided by the interface specified in Chapter 7 of this Technical Specification MUST be supported.		

REQ 240.	Individual checks MUST be stored in the ABC Gates Management server log.		
REQ 241.	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;		

NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**
REQ 242.	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 243.	Error codes of data communication MUST be logged together with timestamp.		
REQ 244.	Document reader SHALL be able to provide all the document verification data in a format that is sufficient to build [BSI-TR-03135-1-v2-1] compatible transaction log, according to XML schemas provided in [BSI-TR-031351-v2-1] p.5.2. Transaction log MUST contain all data obtained in the document verification process, except personal data of a document holder and the MRTD itself.		
REQ 245.	Document verification transaction log MUST be sent to log server of the Contracting Authority.		

NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**

REQ 246.	Biometric verification module SHALL be able to provide all the biometric identification data in a format that is sufficient to build [BSI-TR-03135-1-v2-1] compatible transaction log, according to XML schemas provided in [BSI-TR-03135-1-v2-1] p.5.2. Transaction log MUST contain all data obtained in the biometric identification process, except personal data of a document holder and the MRTD itself.		
REQ 247.	Biometric verification transaction log MUST be sent to log server of the Contracting Authority.		
REQ 248.	Archiving of logs will be agreed with CA during execution of the Contract.		

7 DEFECTS

7.1 OPTICAL DEFECTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 249.	If the defect 'Specimen' applies to the checked document, the document SHOULD be identified and marked as specimen. Further advance through the kiosk workflow must be restricted and the traveller SHALL be instructed to wait for arrival of kiosk operator.		
REQ 250.	If the defect 'Country identifier' applies to the checked document, further advance through the kiosk workflow SHALL be restricted and the traveller SHALL be instructed to wait for arrival of kiosk operator.		
REQ 251.	If the defect 'MRZ format' defect applies to the checked document, further advance through the kiosk workflow SHALL be restricted and the traveller SHALL be instructed to wait for arrival of kiosk operator.		
REQ 252.	If the defect 'MRZ check digit' defect applies to the checked document, further advance through the kiosk workflow SHALL be restricted and the traveller SHALL be instructed to wait for arrival of kiosk operator.		
REQ 253.	If the defect 'MRZ non-IR-readability' defect applies to the checked document, further advance through the kiosk workflow SHALL be restricted and the traveller SHALL be instructed to wait for arrival of kiosk operator.		

7.2 ELECTRONIC DEFECTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 254.	In case of electronic defects further advance through the kiosk workflow SHALL be restricted and the traveller SHALL be instructed to wait for arrival of kiosk operator.		

7.3 BIOMETRIC ENROLLMENTCOMPARISON DEFECTS

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 255.	In case of biometric enrollment or verification failure further advance through the kiosk workflow SHALL be restricted and the traveller SHALL be instructed to wait for arrival of kiosk operator.		

8 DATA/INFORMATION EXCHANGE

8.1 INFORMATION EXCHANGE WITH THE KIOSK OPERATOR DESKTOP WORKSTATION UI

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 256.	Information needed to facilitate the following tasks to be carried out by the operator MUST be supplied: • monitoring the user interface of the kiosk application; • display notifications in case of malfunction or situations except successful check or necessity of kiosk operator arrival to BCP to manage exceptions and make decisions about them;		
REQ 257.	Visual feedback of the enrollment and verification process SHALL be provided for the kiosk operator.		
REQ 258.	At least both facial images (live and reference) SHALL be displayed to the kiosk operator.		
REQ 259.	Captured fingerprint images SHALL be not displayed to the kiosk operator.		
REQ 260.	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 kiosk operator.		
REQ 261.	The result of the biometric verification process SHALL be provided to the kiosk operator's screen.		

REQ 262.	The result of EES enrollment SHALL be displayed to the kiosk operator in EES scenario.		
REQ 263.	Manual override command and sending instructions to traveller to wait for arrival of kiosk operator MUST be supported.		

NO.	**REQUIREMENT DESCRIPTION**	**VENDOR'S RESPONSE**	**FULFILLED**
REQ 264.	The overall verification and enrollment result MUST be displayed in the summary view appearing on the kiosk operator's screen.		
REQ 265.	The image data (VIZ image, DG2 image and live image used for the verification) MUST be shown in the summary view on the kiosk operator's screen.		
REQ 266.	Further details regarding the detailed checks of the biometric verification process SHALL be displayed upon discretion of the kiosk operator.		
REQ 267.	The result of MRZ optical check and comparison ('OK'/'NOK') MUST be displayed on the kiosk operator's screen. Upon discretion of the kiosk operator detailed information SHALL be displayed.		
REQ 268.	The result of eMRTD data verification ('OK'/'NOK') MUST be displayed on the kiosk operator's screen. Upon discretion of the gate operator detailed information SHALL be displayed.		
REQ 269.	A button "Border crossing allowed" for overriding the results of the document /personal identity checks MUST be displayed on the kiosk operator's screen. The button MUST be deactivated in case background check 'NOK' decision will be sent from PIKO.		
REQ 270.	The results of background requests to PIKO ('OK'/'NOK') MUST be displayed on the kiosk operator's screen. Upon discretion of the kiosk operator detailed information SHALL be displayed.		
REQ 271.	An alert in case of an attempt to use a kiosk by a minor MUST be displayed on the kiosk operator's screen.		
REQ 272.	An alert in case of a PAD attack MUST be displayed on the kiosk operator's screen.		
REQ 273.	Alerts MUST be displayed on the kiosk operator's screen: • in case of technical malfunction (missing communication with document reader, …); etc.		

REQ 274.	A notice about a traveller required manual control MUST be displayed on the kiosk operator's screen.		
REQ 275.	A notice about kiosk manual override activated MUST be displayed on the kiosk operator's screen.		
REQ 276.	The kiosk operator desktop workstation UI SHALL be operating in Windows 10 Pro environment.		
REQ 277.	The solution of authentication and authorisation of the kiosk operator desktop workstation UI SHALL be agreed with the Contracting Authority during execution of the Contract.		

8.2 INFORMATION EXCHANGE WITH THE KIOSK OPERATOR MOBILE UI

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 278.	The overall verification result MUST be displayed in the summary view appearing on the kiosk operator's mobile screen.		
REQ 279.	The result of the biometric verification process (OK/not OK) MUST be displayed to the kiosk 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 kiosk operator.		
REQ 280.	The result of MRZ optical check and comparison (OK/not OK) MUST be displayed on the kiosk operator's mobile screen. Upon discretion of the kiosk operator detailed information SHALL be displayed.		
REQ 281.	The result of eMRTD data verification (OK/not OK) MUST be displayed on the kiosk operator's mobile screen. Upon discretion of the kiosk operator detailed information SHALL be displayed.		
REQ 282.	A button "Border crossing allowed" for overriding the results of the document /personal identity checks MUST be displayed on the kiosk operator's screen. The button MUST be deactivated in case 'NOK' decision will be sent from PIKO.		
NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 283.	The results of background requests to PIKO (OK/not OK) MUST be displayed on the kiosk operator's mobile screen. Upon discretion of the kiosk operator detailed information and workflow SHALL be displayed.		

REQ 284.	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 kiosk operator's mobile screen.		
REQ 285.	An alert in case of an attempt to use a kiosk by a minor MUST be displayed on the kiosk operator's mobile screen.		
REQ 286.	Alerts MUST be displayed on the kiosk operator's mobile screen: • in case of technical malfunction (missing communication with document reader, …); etc.		
REQ 287.	A notice about kiosk manual override activated MUST be displayed on the kiosk operator's mobile screen.		
REQ 288.	The result of EES enrollment/verification SHALL be displayed to the kiosk operator in EES scenario.		
REQ 289.	The solution of authentication and authorisation of the kiosk operator mobile UI SHALL be agreed with the Contracting Authority during execution of the Contract.		

8.3 INSTRUCTIONS FOR A TRAVELLER

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 290.	Full guidance MUST be provided on the kiosk screen. The contents of the guidance, e.g. looping video, SHALL be coordinated with CA.		
REQ 291.	An indicator showing the capture status SHOULD be displayed to the passenger.		
REQ 292.	Information whether a kiosk is operational or not MUST be displayed to the travellers in clear and understandable form.		
REQ 293.	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 Contracting Authority during execution of the Contract.		
REQ 294.	Audio instructions for the traveller MAY be provided.		

REQ 295.	The information for the traveller 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 CA.		
REQ 296.	Graphics on the traveller's UI screen should avoid multiple colours or harsh contrast.		
REQ 297.	A correspondence table containing system messages and respective messages to the traveller MUST be present in the ABC Gates management server. The contents of this table SHALL be agreed with the Contracting Authority during execution of the Contract.		

8.4 Data exchange with PIKO

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 298.	In case of non-EES scenario the following data MUST be delivered to PIKO: • Contents of MRZ;		
REQ 299.	In case of EES scenario the following data MUST be delivered to PIKO: • Contents of MRZ; • EES compliant Face image • EES compliant Fingerprint images		
REQ 300.	In case of EES scenario PIKO delivers to kiosk management system: • Information about required workflow: Verification or Identification • Matching result(s) from EES central system for verification or identification		

9 REQUIREMENTS TO SECURITY OF THE SOLUTION

9.1 Securing the communication

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 301.	In order to secure the communication channel of the transmission, the use of either TLS 1.2 or 1.3 [RFC5246] MUST be supported.		
REQ 302.	No other network connection except to the CA's network SHALL be used.		
REQ 303.	Data exchange with kiosk SHALL be protected from electronic and mechanical interception.		

10 REQUIREMENTS TO SERVICE LEVEL AGREEMENT

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 304.	All requirements SHALL be applicable per kiosk. Temporal requirements can't be consolidated.		

10.1 Key performance Indicators

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 305.	Yearly uptime per kiosk MUST be 99 (ninetynine) per cent.		

11 Additional information

11.1 EAC and Fingerprint Enrollment

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 306.	The service SHALL be delivered with readiness to implement fingerprint check and EAC functionality on short notice.		

11.2 List of messages to kiosk operator

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 307.	The messages to kiosk operators will be agreed with CA during execution of the Contract.		

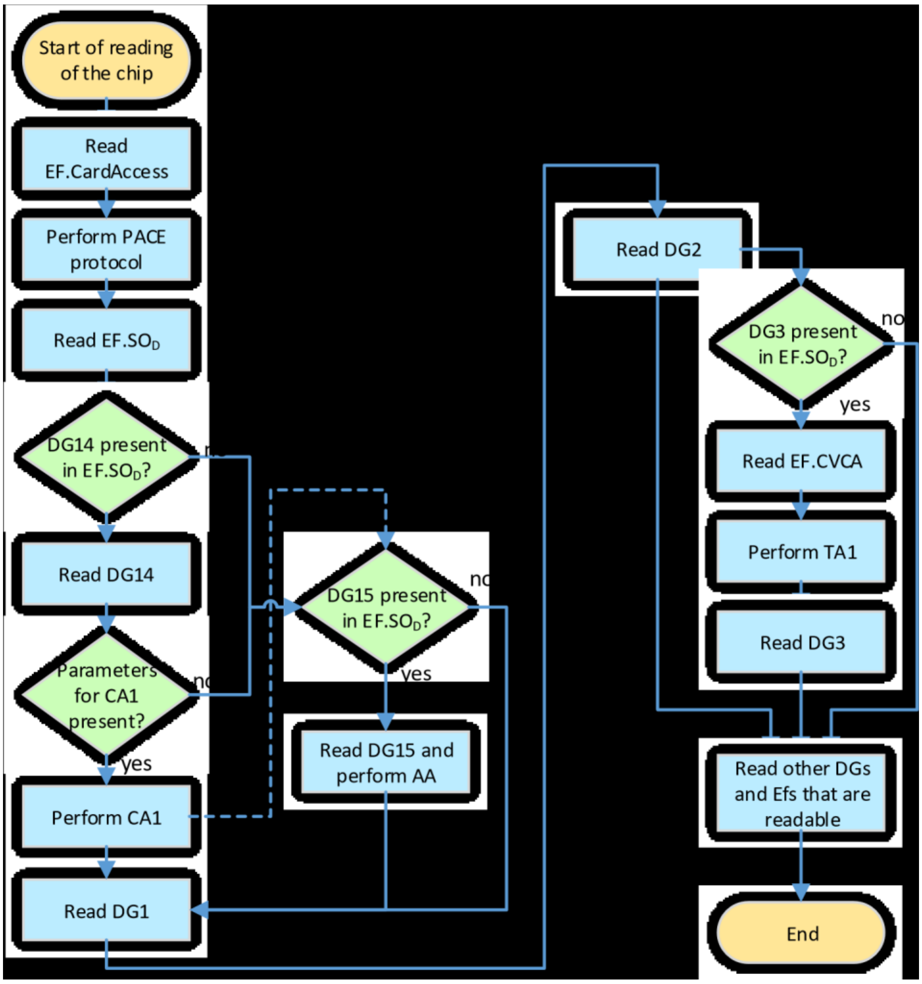
11.3 LIST OF MESSAGES TO A TRAVELLER

NO.	REQUIREMENT DESCRIPTION	VENDOR'S RESPONSE	FULFILLED
REQ 308.	The messages to traveller will be agreed with CA during execution of the Contract.		

12 ANNEX 2. FUNCTIONALITY UPGRADES

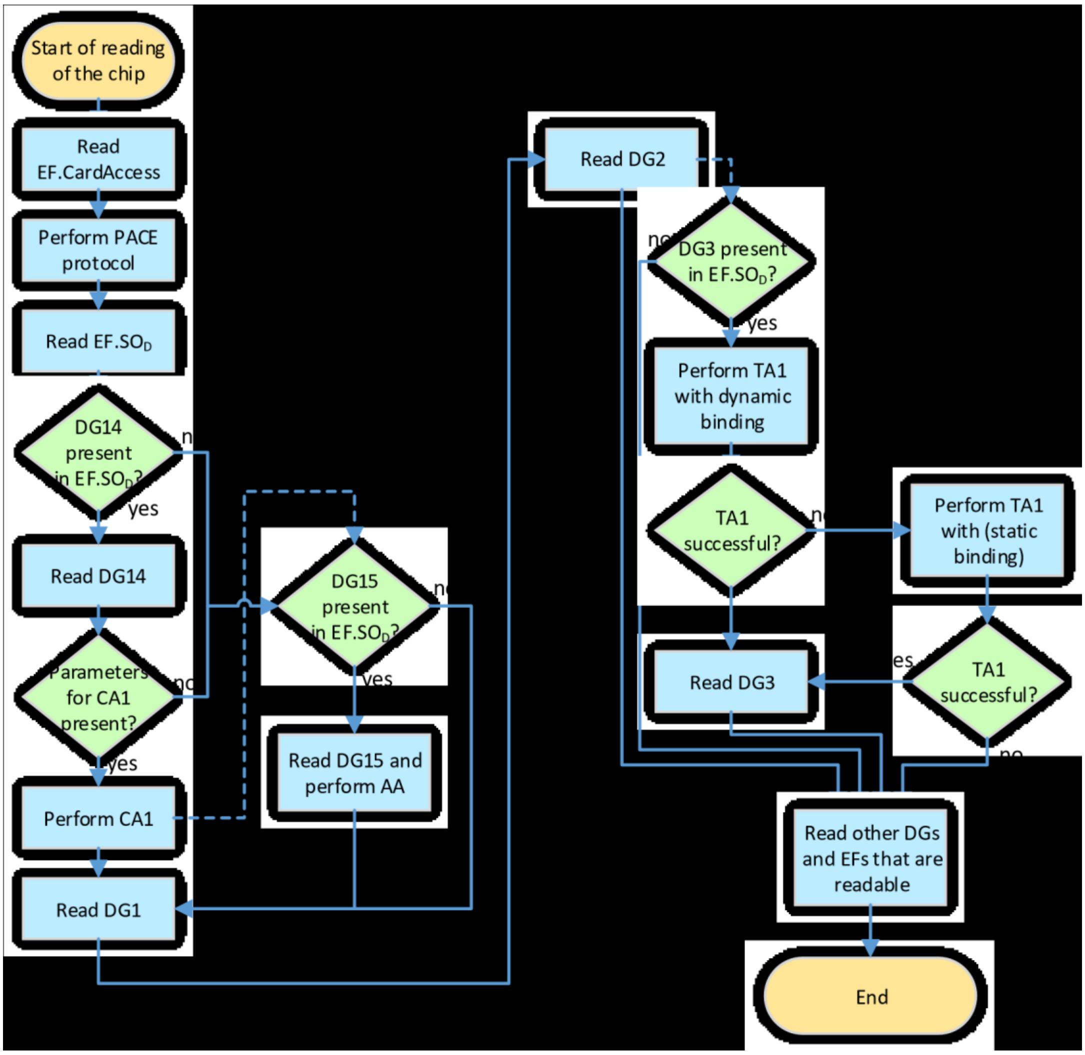
This Clause is informative at the moment of publishing this Tender and is intended to inform the Vendor about the scope of the future functionality upgrades to the system. These upgrades MUST be supported during this tender and they will be activated concurrently with implementation of EAC functionality.

12.1 CHANGES IN ELECTRONIC CHECKS PROTOCOL SEQUENCES



Start of reading of the chip
Read EF.CardAccess
Perform PACE protocol
Read EF.SO$_D$
DG14 present in EF.SO$_D$?
Read DG14
Parameters for CA1 present?
no
yes
Perform CA1
Read DG1
DG15 present in EF.SO$_D$?
no
yes
Read DG15 and perform AA
Read DG2
DG3 present in EF.SO$_D$?
no
yes
Read EF.CVCA
Perform TA1
Read DG3
Read other DGs and Efs that are readable
End

Figure 11: Protocol Sequence 1, performing BAC



Start of reading of the chip
Read EF.CardAccess
Perform PACE protocol
Read EF.SO$_D$
DG14 present in EF.SO$_D$?
no
yes
Read DG14
Parameters for CA1 present?
no
yes
Perform CA1
Read DG1
DG15 present in EF.SO$_D$?
no
yes
Read DG15 and perform AA
Read DG2
DG3 present in EF.SO$_D$?
no
yes
Perform TA1 with dynamic binding
TA1 successful?
no
Perform TA1 with (static binding)
TA1 successful?
yes
no
Read DG3
Read other DGs and EFs that are readable
End

Figure 12: Protocol Sequence 2, performing PACE, CA1 or AA

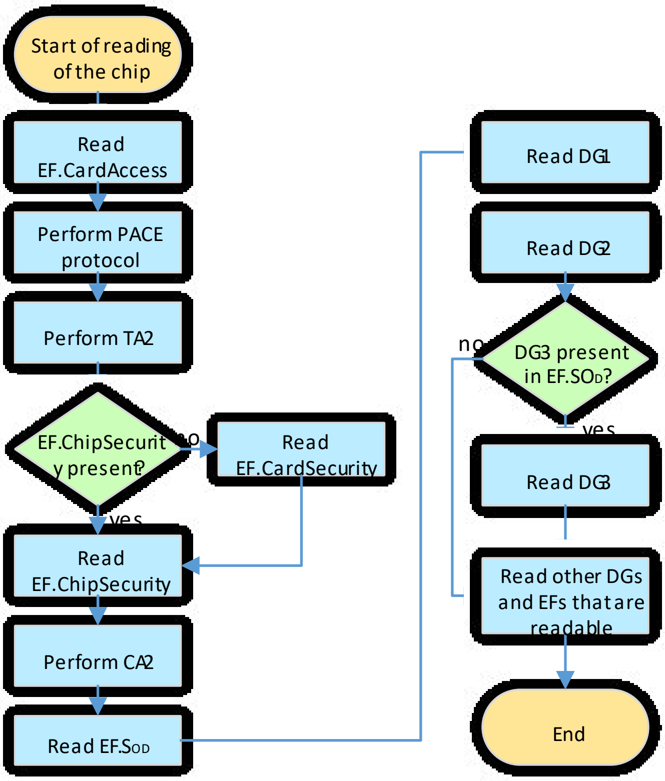


Figure 13: Protocol Sequence 3, performing PACE, TA2, CA2

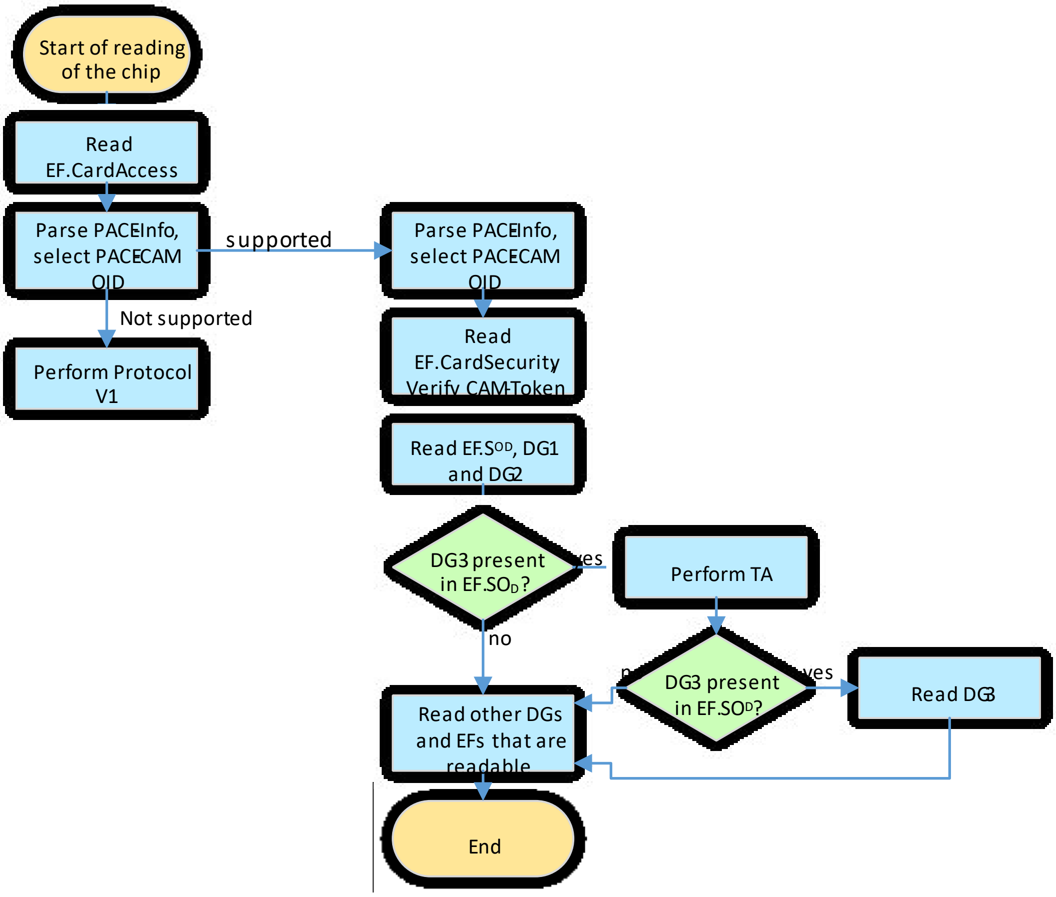

Start of reading of the chip
Read EF.CardAccess
Parse PACEInfo, select PACECAM OID
supported
Not supported
Perform Protocol V1
Parse PACEInfo, select PACECAM OID
Read EF.CardSecurity Verify CAM-Token
Read EF.SOD, DG1 and DG2
DG3 present in EF.SOD?
yes
no
Perform TA
DG3 present in EF.SOD?
no
yes
Read DG3
Read other DGs and EFs that are readable
End

Figure 14: Protocol Sequence 4, support of PACE-CAM

12.2 Changes due implementing MasterLists, DefectLists etc.

No.	Requirement Description	Vendor's Response	Fulfilled
REQ 309.	CDS will be sent to RCC and reply will be returned to the IS.		
REQ 310.	Access to RCC will be available via VPN to the specified network address/port in the Contracting Authority's network.		

13 REQUIREMENTS DEFINITION AND TENDER EVALUATION

13.1 Requirements Definition

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

13.1.1 Minimum 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.