



Î.C.S. "Reliable Solutions Distributor" S.R.L.  
Chișinău, str. Alexandru cel Bun, 85, MD-2012  
Tel: +373 78857746 | Email: [office@rsd.md](mailto:office@rsd.md)

## **Sistem automatizat al controlului de frontieră (Automated Border Control, ABC, e-Gate)**

**Către: Î.S. „Aeroportul Internațional Chișinău”,**  
**mun.Chișinău, bd. Dacia, 80/3, MD-2026**  
MTender ID - ocds-b3wdp1-MD-1751977966815

## Table of Contents

<b>1</b>	<b>DESCRIPTION OF BASIC FUNCTIONALITIES FOR AUTOMATED BORDER CONTROL (ABC, E-GATE) ....</b>	<b>4</b>
<b>2</b>	<b>AUTOMATED BORDER CONTROL E-GATES.....</b>	<b>13</b>
2.1	Executive Summary .....	13
2.2	Technical Description of the eGate Solution .....	15
2.2.1	Basic Double Door FastGate .....	15
2.3	MB Fast Gate - Hardware .....	16
2.3.1	Material .....	16
2.3.2	UPS.....	17
2.3.3	PC .....	17
2.3.4	Swing Doors .....	18
2.3.5	Side Walls .....	18
2.3.6	Sensors, alarms & security .....	18
2.3.7	Key Switch .....	18
2.3.8	Led indicators .....	19
2.3.9	Modularity .....	19
2.3.10	Document Reader.....	19
2.3.11	Dual Interface Smartcard Reader.....	25
2.3.12	Biometric face camera.....	25
2.3.13	Monitor/Display .....	25
2.3.14	CCTV .....	26
2.3.15	Installation .....	26
2.3.16	SDK for Bio Devices and Gate Control .....	26
2.4	MB Fast Gate – Software / Control and Monitoring of the ABC System .....	27
2.4.1	Border Guard Control Unit (MB BGCU).....	28
2.4.2	Passenger passes process.....	31
2.4.3	Border Management Adapter (MB BMA).....	31
2.4.4	MB Trust Inspection System.....	32
2.4.5	MB User Management .....	32
2.4.6	MB Audit .....	33
2.4.7	Liveness Detection System .....	33
2.5	Deliverables for ABC e-gates HW & SW.....	34
<b>3</b>	<b>SERVICES FOR ABC E-GATES .....</b>	<b>36</b>
3.1.1	Project Initiation .....	36
3.1.2	Pre-Commissioning at the supplier Facility (Mühlbauer) .....	36
3.1.3	Training for customer at Mühlbauer Facility .....	36
3.1.4	Factory Acceptance Test (FAT) .....	36
3.1.5	Logistics .....	37
3.1.6	Installation and commissioning at Chisinau Airport, Moldova .....	38
3.1.6.1	Customer testing and validation .....	38
3.1.7	Training for customer at Customer Facility .....	38
3.1.8	Site Acceptance Test (SAT) .....	38
3.1.9	Ramp-up Support.....	38
3.2	Maintenance and Support Services.....	39
3.2.1	Corrective Maintenance .....	39
3.2.1.1	1st Level Support: Technical Support Group (TSG) .....	39
3.2.1.2	2nd Level Support (Remote Support) .....	39
3.2.1.3	3rd Level Support (Remote Support).....	39

3.2.1.4	Field Service Support.....	39
3.2.2	Preventive Maintenance .....	39
3.2.2.1	Preventive Maintenance for eGates.....	39
3.2.2.2	Remote Preventive Maintenance for eGates Software Components .....	40
3.2.3	Software Subscriptions .....	40
3.2.4	Warranty - Supply of Spare Parts.....	40

# 1 Description of basic functionalities for Automated Border Control (ABC, e-Gate)

Requirement	Compliance
The ABC system shall provide travelers with a fully automated, self-service border control crossing, fulfilling full travel document verification and facial biometric identification of passenger identity, in accordance with the Frontex Agency's requirements on 'Best Practice Technical Guidelines for Automated Border Control (ABC) Systems'.	
<b>1. General requirements for the ABC System</b>	
1.1. The construction of the overall ABC System shall be in accordance with applicable ICAO and IATA recommended practices;	Compliant Please ref. chapter 2.2.1
1.2. The construction of the ABC System shall be with 2 barriers/ gates (entry and exit) performing two-stage screening of the person. Each stage shall include a barrier with double gates;	Compliant Please ref. chapter 2.2.1
1.3. The ABC System construction shall include features (including required sensors) to ensure that there will be no tailgating or crossovers during the process of passing through the ABC System;	Compliant Please ref. chapter 2.4, chapter 2.4.2
1.4. Full hardware modularity for single-row or multi-row gate configuration	Compliant Please ref. chapter 2.3.9
1.5. Sensors shall be placed to detect and warn passengers of remaining objects (e.g. baggage, etc.) in the ABC System control area;	Compliant Please ref. chapter 2.3.6
1.6. The construction of the ABC System should be an open design that avoids the feeling of confinement and claustrophobia and provides optimal visibility for the inspector;	Compliant Please ref. chapter 2.2.1
1.7. The exit barrier must be of sufficient height so that the passenger who needs to pass the classical (counter) border check cannot bypass or jump;	Compliant Please ref. chapter 2.3.4 chapter 2.3.5
1.8. The construction of the ABC System must be safe for passengers, such as avoidance of sharp objects/elements, smooth finishes, curved edges, etc.;	Compliant Please ref. chapter 2.3.4 chapter 2.3.5
1.9. All materials used in the ABC System must be certified for use in aviation terminals in terms of safety and health standards;	Compliant Please ref. Chapter 2.3.1
1.10. All electronic and mechanical components (such as circuit boards, motorized hinges, etc.) shall be concealed where possible and shall be secure;	Compliant Please ref. chapter 2.2.1
1.11. The construction of the ABC System shall be resistant to vandalism, scratches and protected against foreign materials such as chewing gum, beverages, spilled water, cleaning fluids, etc.	Compliant Please ref. chapter 2.3.1
1.12. In order to protect biometric data and travel documents processed by the ABC System, the Provider shall comply with the following minimum security requirement cyber: a) all communications between the ABC System and the IGPF's IT infrastructure (including web services) will be secured via TLS 1.2 or higher protocols, using digital certificates issued by a recognized certification authority;	Compliant Please ref. chapter 2.4.9 2.4.3
b) access to the administration interface and monitoring stations will be protected by multi-factor authentication (MFA) and role-based access control (RBAC) policies;	Compliant Please ref. chapter 2.4.5

c) all logged and locally captured data (images, logs, events) shall be encrypted at disk level (AES-256 or equivalent), with configurable retention period;	Compliant Please ref. chapter 2.4.9
d) the supplier shall ensure that all software components comply with the principles of "secure-by-design and will be subject to penetration testing and security audit;	Compliant Please ref. chapter 2.4
e) the ABC system, including its software and hardware components, must comply with the requirements of Regulation (EU) 2016/679 (GDPR);	Compliant Please ref. chapter 2.2.1
f) the provider shall provide evidence of compliance with the ISO/IEC 27001 standard for information security management.	Compliant Please refer to attached ISO 27001 certificate
<b>2. General requirements for operating the ABC System</b> Citizens of the Republic of Moldova who have reached the age of 18 years and are not accompanying minors are the basic eligible category to cross the state border through the ABC System. Depending on the evolution of the regulatory framework, the General Inspectorate of the Border Police will decide which citizens are eligible to use the ABC System. In this regard, the ABC System should provide the flexibility and technical possibility to expand the categories of persons who can cross the state border using the ABC System.	
2.1. The process of the ABS transition (steps, actions/processes, information, communication API, informative messages, others) will be jointly developed between the Beneficiary and the Bidder, but at the same time the Bidder will describe at least 2 different processes (transition processes used in other implemented projects, best practices);	Compliant Please ref. chapter 2.4.2
2.2. The communication between the ABC system and the IGP data and application server must be via SOAP web services;	Compliant Please ref. chapter 2.4.1
2.3. The information processes (applications) within the ABC System shall save audit/recording data for all actions taking place in the border control crossing process. The audit/reporting data (in the form of files stored locally on the ABC System processor disk) shall be kept for a maximum of 7 days;	Compliant Please ref. chapter 2.4.6
2.4. Control/documentation requirements against the ABC System entry process: The first barrier (entry gates) of the ABC System shall support the following operations/documentation:	Compliant Please ref. chapter 2.3.10
2.4.1. A biometric travel document reader, minimum technical requirements <i>Annex 2</i>	
2.4.2. A monitor/tablet (small size) designed to display information to guide the passenger through the biometric travel document reading process and display results (such as eligibility for ABC System use, etc.) based on information received from the ABC System;	Compliant Please ref. chapter 2.3.13 Chapter 2.4.2
2.4.3. Entry barrier (2 gates that open forward) and sensors that ensure that only one person enters the second stage (in the "trap/work" area for persons) when entry is permitted. The minimum technical requirements for the sensors are described under 'Safety and security';	Compliant Please ref. chapter 2.3.6
2.5. Control/documentation requirements to the ABC System output process: The second barrier (exit gates) of the ABC System shall support the following operations/documentation:	Compliant Chapter 2.4.2
2.5.1. Passenger face image capture hardware/software system with the following minimum technical requirements (ICAO compliant):	
2.5.1.1. "active life" detection based on 3D imaging technology;	Compliant Please ref. chapter 2.4.7
2.5.1.2. Facial image capture shall support (automatically adjusting) the variable height of the passenger and be capable of capturing the image when the passenger is standing;	Compliant Please ref. chapter 2.3.12

2.5.1.3. The system shall be equipped with a 'digital mirror' to assist the passenger during image capture. The passenger shall also receive the necessary instructions on a monitor/screen including graphic instructions. All information provided shall be in accordance with user-friendly practices;	Compliant Please ref. chapter 2.3.12
2.5.1.4. The face capture algorithm must continuously analyze the video stream from the camera to detect the passenger's face. As soon as the passenger's face is detected at the correct distance from the camera, it shall run a quality assessment algorithm (computer process) to verify that the face image meets the minimum criteria based on ISO 39794-5 and ISO/IEC 19794-5:2011 "Face image (eye distance, blur, focus, pose, expression)";	Compliant Please ref. chapter 2.4.2
2.5.1.5. The system shall be equipped with an identity theft protection system, "Anti-spoofing control", which will prevent attempts to submit facial images, photographs or videos;	Compliant Please ref. chapter 2.4.7
2.6. The system shall have an emergency switch/button that allows the passenger to request assistance from the inspector. The emergency switch shall trigger an alarm (audible and visible) but shall not automatically release the barriers. The inspector shall be able to open the entry barrier using an 'emergency button', which shall not be accessible to the passenger at the second stage of the check;	Compliant Please ref. chapter 2.4.1
2.7. Information system for managing/operating with all IT processes related to border crossing control in the ABC System shall be provided with a large set of configurations for all stages.	Compliant Please ref. chapter 2.4.9
<b>3. Safety and security</b>	
3.1. The ABC System must have sensors that are able to detect a number of security related conditions/concerns including:	
3.1.1. The ability to differentiate an adult or child walking, plus carry-on luggage, plus suitcases and wheeled bags (pulling or pushing);	Compliant Please ref. chapter 2.3.6
3.1.2. The ability to detect multiple people (presence sensors, adult, child, adult with child in arms) entering the security zone - tailgating;	Compliant Please ref. chapter 2.3.6
3.1.3. Capability on full tailgating detection functionality (no additional camera above), based on artificial intelligence integrated into the vision system.	Compliant Please ref. chapter 2.3.6
3.1.4. Ability to have radar sensors integrated in the bottom for scanning door areas.	Compliant Please ref. chapter 2.3.6
3.1.5. Ability to detect multiple passengers inside the ABC System (Presence Sensors), including adults with minors in their arms;	Compliant Please ref. chapter 2.3.6
3.1.6. Ability to detect attempts to force open entry and exit doors;	Compliant Please ref. chapter 2.3.6
3.1.7. Ability to detect a passenger traveling in the wrong direction;	Compliant Please ref. chapter 2.3.6
3.1.8. The ability to detect luggage or other unexpected objects left inside.	Compliant Please ref. chapter 2.1, chapter 2.4.1 chapter 2.3.6
3.2. <b>Optional:</b> The ABC System shall be equipped with CCTV cameras to provide the inspector with a clear view of the entire process of passing through the ABC System;	Compliant Please ref chapter 2.3.14
3.3. The System shall have a "Visual Signage" system that provides color coded visual signage displaying the operational status of the System, such as waiting for next passenger, busy, inoperative (maintenance mode), alarm, etc. The color coding shall be determined in consultation	Compliant Please ref. chapter 2.1

with the Beneficiary. "Visual signaling" may be through the use of monitor/screen (small size) which requires to be installed at the first barrier;	
3.4. The ABC system shall be designed to provide an average processing time of maximum 20 seconds per passenger;	Compliant Please ref. chapter no 2.1
<b>4. Control and monitoring of the ABC System</b>	
4.1. The ABC System shall be equipped with a live monitoring station, located in a kiosk close to the ABC Systems. The monitoring station shall provide a detailed overview of the operational status of each ABC System and its performance data. <b>Optional:</b> the control panel shall include a video monitoring component providing live images from CCTV cameras installed in/on the ABC Systems;	Compliant Please ref. chapter 2.4.1, chapter 2.4.2, and chapter 2.3.14
4.2. The monitoring station shall allow the inspector to monitor and control a group of ABC Systems from a single workstation. A monitoring station shall allow the inspector to view and manage up to 5 Systems at the same time;	Compliant Please ref. chapter 2.4.1
4.3. The monitoring stations shall be provided by the Bidder - 2 sets (system block, monitor, keyboard, keyboard, mouse, connecting cables, UPS, licensed software);	Compliant
4.4. Through the Monitoring Station, the inspector shall have full control of the ABC System and shall be able to open both entry and exit doors (the door will close automatically when time expires or after the passenger has passed), reset/restart and activate/deactivate the ABC System;	Compliant Please ref. chapter 2.4.1
4.5. To ensure efficient operation of the ABC System within the airport ecosystem, the Supplier shall detail in its technical proposal the following: <b>a)</b> How to integrate with existing systems including: • DCS (Departure Control System); • AODB (Airport Operational Database); • FIDS (Flight Information Display System); • RMS (Resource Management System).	Compliant Please ref. chapter 2.4.1
<b>b)</b> the proposed logical integration architecture, including data exchange (format, frequency, protocols) and fallback mechanisms in case of unavailability of external systems;	Compliant Please ref. chapter 2.4.3
<b>c)</b> clarification of the responsibilities for the connection and operation of the respective interfaces.	Compliant Please ref. chapter 2.4.1
4.6. Power on/off function with hidden switch (key).	Compliant Please ref. chapter 2.3.7
4.7. The main features of the monitoring workstation shall be: 4.10.1. Visualization of the data retrieved from the biometric travel document, including the face image from the CIP and the visual zone (VZ, from the data page);	Compliant Please ref. chapter 2.4.1
4.10.2. Visualization, when necessary, of the images scanned by the travel document reader in all possible light spectra;	Compliant Please ref. chapter 2.4.1 and 2.3.10
4.10.3. Monitor and control the automatic facial recognition process, including viewing live captured images of the passenger and the possibility to perform manual recognition if necessary;	Compliant Please ref. chapter 2.4.2
4.10.4. In case of unsuccessful identity verification: possibility to configure the system behavior - either the person is forced to leave the gate or is detained until released by an officer.	Compliant Please ref. chapter 2.3.6
4.10.5. Possibility to release the person via key switch (separate for each line) or via border control software.	Compliant Please ref. chapter 2.4.1
4.10.6. Visualization of the results of the facial recognition procedure. When the facial recognition score falls below the specified minimum value, the application displays alerts;	Compliant Please ref. chapter 2.4.1
4.10.7. View live video images from the facial camera;	Compliant

	Please ref. chapter 2.4.1
4.10.8. Real-time monitoring of border control crossing processes, including ABC System status;	Compliant Please ref. chapter 2.4.1 and chapter 2.4.2

4.10.9. Alerting on alarm conditions and other notifications (e.g. tracking, abandoned objects).	Compliant Please ref. chapter 2.3.6
<b>5. Training</b>	
5.1. The Tenderer shall conduct appropriate training for the Beneficiary's technical team on maintenance, how to troubleshoot and remove insignificant errors (software and hardware);	Confirmed
5.2. The Provider shall provide user manuals and technical documentation during the implementation of the ABC Systems.	Confirmed
<b>6. Maintenance and support requirements</b>	
6.1. The Offeror shall provide a detailed preventive and corrective maintenance plan for the ABC Systems, including regular maintenance intervals and troubleshooting procedures;	Confirmed
6.2. The Offeror shall provide spare parts for all essential ABC System components for the entire warranty period and for post-warranty maintenance;	Confirmed
6.3. If a major malfunction is identified that affects the normal operation of the ABC System, the Offeror will be required to intervene to remedy the fault within a timeframe set out in the support agreement, typically no more than 72 hours;	Confirmed
6.4. The Offeror shall provide ongoing training for the Beneficiary's technicians during the use of the ABC System to ensure its efficient operation and safety.	Confirmed
<b>7. Commissioning and periodic validation tests</b>	
7.1. Full system functionality testing (document capture, facial identification validation, barrier access control, etc.);	Confirmed
7.2. Performance testing to check processing time and passenger throughput per minute;	Confirmed
7.3. All tests will be documented in a test report to be submitted to the Beneficiary for validation.	Confirmed
7.4. To validate the interoperability, performance and compatibility of the ABC System with the existing infrastructure:	Confirmed
a) The vendor will implement a functional pilot installation for a minimum of 1 ABC gate, including integration with IGPF infrastructure and testing of biometric capabilities;	
b) the testing period will be a minimum of 30 days, with documentation of all results and possible non-conformities;	Confirmed
c) Full commissioning of the other units will be conditional on formal acceptance of the PoC results by the Beneficiary.	Confirmed
<b>8. Compliance Requirements</b>	
8.1. All components of the ABC System shall comply with ICAO (International Civil Aviation Organization) and IATA (International Air Transport Association) regulations;	Compliant Please ref. chapter 2.3.10
8.2. The system shall be certified for use in airport terminals, complying with safety regulations and fire safety standards.	Compliant Please ref. chapter 2.1
8.3. The supplier shall provide full documentation on the API structure used by the ABC System (methods, parameters, responses, error codes, authentication);	Compliant Please ref. chapter 2.4.3
8.4. The functional and safety test methods applicable to the API shall be specified;	Compliant Please ref. chapter 2.4.3
8.5. The Supplier shall present a rollback plan in case of critical failure after an upgrade of the ABC software (including backups, rollback procedures, estimated duration).	Confirmed
<b>9. Delivery and implementation timelines</b>	
9.1. The Supplier shall provide a detailed schedule for delivery, installation and commissioning of the ABC Systems, including milestones and timelines for completion;	Confirmed

9.2. The maximum deadline for the installation and full commissioning of the ABC Systems is 6 months from the signing of the contract;	Confirmed
<b>10. Reporting and documentation requirements</b>	
10.1. The Provider must provide detailed reports on project progress, testing and validation updates, and any delays or problems that may occur during implementation;	Confirmed
10.2. All documents and reports must be provided in English and Romanian;	Confirmed
10.3. Upon completion of the implementation, the supplier shall deliver the complete documentation on system architecture, operational procedures, user manuals and maintenance guides.	Confirmed
<b>11. Final Beneficiary Obligation (General Inspectorate of Border Police)</b>	
12.1. The IGPF will publish a set of APIs (SOAP web services) to be consumed/accessed by the ABC System for the authorization of automated border control crossing by the passenger.	Compliant Please ref. chapter 2.4.3
<b>12. Log retention policy</b>	
12.2. The ABC system will retain logging data (system logs, access logs, captured images) for a minimum of 30 days, with the possibility of automatic extension or archiving;	Compliant Please ref. chapter 2.4.6
12.3. Secure deletion policies will be configurable in accordance with the internal policies of the Beneficiary and GDPR provisions.	Compliant Please ref. chapter 2.4.6
<b>Annex 2</b>	
<b>Minimum technical requirements for the biometric travel document reader device</b>	
Device for automatic reading of the whole data page of the biometric travel document, without removable parts, intended for reading data from: machine readable zone (MRZ); visual zone (VZ); wireless electronic identification circuit (RFID); bar code, comparison of read data, verification of the authenticity of the travel document by the possibility of scanning the data page under different light spectra (White, IR, UF, coaxial, OVD, others).	Compliant Please ref. chapter 2.3.10
<b>Optical document reader</b>	
Scanning area - the whole page of the passport; Video sensor type - CMOS; Color representation - RGB Color depth - 24 bits Number of megapixels - 18, with the possibility to set values from a list. The list must contain at least 3 values ranging from 1..5, 5..10, 10..18;	Compliant Please ref. chapter 2.3.10
<b>Contactless electronic identification circuit reader:</b>	
Standards - ISO 14443: A and B for RFID-electronic circuits; Information exchange rate - 106, 212, 424, 848 Kbaud Reading of electronic circuits - RFID placed in any part of the travel document Anticollision: detection/reading of RFID electronic circuit after reading the machine readable zone (MRZ)	Compliant Please ref. chapter 2.3.10
<b>Reading and image processing of documents format:</b>	
ID-1, ID-2, ID-3 and other documents that do not exceed 88x128 mm in size; Scanning process: Determining the existence in the document reader after the sensor Automatic scanning of the document after the document has been detected; Elimination of reflective (glare) lights from laminate and holograms for white and infrared light spectrum; Compensating the exposure of external light when capturing (shooting) images in the ultraviolet light spectrum (Smart UV); Automatic selection of ultraviolet illumination intensity for the type of documents being processed; Determine (search) and select images (photo, MRZ, signature, data fields) from the total document image.	Compliant Please ref. chapter 2.3.10

<p><b>Machine Readable Zone (MRZ)</b>        Supported formats of the machine readable zone (MRZ) according to ICAO standard 9303s. Search for the mechanizable zone on the document image;        Recognition in the white and infrared light spectrum;        Verification of check digits to verify the correct completeness of the machine-readable area according to ICAO 9303 requirements.        Evaluation of the correctness and quality of printing in accordance with ICAO 9303 и ISO 7501, 1831, 1073-2 standards.</p>	<p>Compliant        Please ref. chapter 2.3.10</p>
<p><b>Barcode reading:</b>        Maintained formats:        1D: Codeabar, Code39 (+extended), Code93, Code128, EAN-8, EAN-13, IATA 2 of 5 (Airline), Interleaved 2 of 5 (ITF), Matrix 2 of 5, STF (Industrial), UPC-A, UPC-E        2D: PDF417, Aztec Code, QR Code, Datamatrix</p>	<p>Compliant        Please ref. chapter 2.3.10</p>
<p><b>Automatic document type determination</b>        Document type determination sequence Country→Type→Series        Receive from the SDK database the document template for further processing:        - location of text and graphic fields;        - existence of barcodes and protection elements;        - authenticity check and its parameters;        - existence of electronic circuits - RFID.</p>	<p>Compliant        Please ref. chapter 2.3.10</p>
<p><b>RFID SDK/Functionality</b>        Supported standards for electronic circuits - RFID:        - ISO/IEC 14443-2 (type A and B)        - ISO/IEC 14443-4        Data access regime: Direct, BAC, EAC, PACE        Authentication:        Active (AA)        Passive (PA)        electronic circuit (CA v1, CA v2) terminal (TA v1, TA v2)        Application support:ePassport (DG1-DG16), eID (DG1-DG21), eSign;        Certificate management:        Local storage;        Getting certificates on-line via software interface; Master List, CRL support        Reading with Extended Length Support        Reading contactless electronic circuits according to ICAO LDS 1.7, PKI 1.1 data formats</p>	<p>Compliant        Please ref. chapter 2.3.10</p>
<p><b>Required mandatory security functionality:</b>        - Full tailgating detection functionality (without additional overhead camera) based on artificial intelligence integrated into the vision system.        - Bottom integrated radar sensors for scanning door areas.        - Full hardware modularity for single-row or multi-row door configuration.        - Power on/off function with hidden key switch.        - In case of unsuccessful identity verification: possibility to configure the system behavior - either the person is forced to leave the gate or is detained until released by an officer.        - Possibility to release the person via key switch (separate for each line) or via the border control software interface.</p>	<p>Compliant        Please ref. chapter 2.3.6</p>
<p><b>Analysis and comparison of textual information</b>        Areas of the document whose data will be analyzed (compared):        - machine-readable area        - visual area        - RFID electronic circuit</p>	<p>Compliant        Please ref. chapter 2.3.10</p>

<p><b>Authenticity verification</b></p> <ul style="list-style-type: none"><li>- Luminescence check (UV Dull Paper): banquette, MRZ, photo location area;</li><li>- MRZ print contrast check in accordance with ICAO standard 9303 (IR B900 Ink) Checks available after document type determination:</li><li>- Check for patterns of certain colors and shapes in the white, infrared and ultraviolet light spectrum (Image Pattern);</li><li>- check the illumination of fibers of a certain color and size (UV Protection Fibers)</li><li>- checking for False Luminescence (False Luminescence)</li><li>- Checking the method of photo embedding: printing or pasting (Photo Embedding Type)</li></ul> <p>Checking the visibility in the infrared spectrum (IR Visibility):</p> <ul style="list-style-type: none"><li>- white elements</li><li>- textual data</li><li>- photo (basic and additional)</li><li>- checking for holograms (OVD)</li><li>- reading luminescent text and comparing with data read from the machine readable zone MRZ or visual area VIZ (OCR Security Text)</li><li>- Invisible Personal Information (IPI) visualization</li><li>- checking retro reflective protection</li><li>- bar code format verification.</li></ul>	<p>Compliant Please ref. chapter 2.3.10</p>
---	---

## 2 Automated Border Control e-Gates

### 2.1 Executive Summary

Effective immigration and border management is vital to increase efficiency and security at airports, land borders and seaports especially when passenger volumes increase due to travel season or public events such as Olympic Games or world soccer championship.

One major element for efficient border management is facilitation of automated border control (ABC) systems, such as eGates & Kiosks.

In this document, the offered MB Fast Gate follows modular design principles. This allows almost arbitrary Gate setups and topologies.

Compliance to relevant international standards was another major objective of the Gate design. Thus the offered solution complies with national regulations, such as German BSI standards, ANSI ANSI/T1.101-1987, National Electrical Manufacturers Association (NEMA), National Electrical Safety Code (NEC), ISO standards ranging from ISO 7810, 7816 related to smart cards, electronic documents, RFID, LDS etc. to the biometric data format specified in ISO 17497 - X, International Civil Aviation Organization (ICAO) regulations, especially recommendation from Doc 9303 are applied to assure 100% electronic travel document interoperability. Other standards, such as International Air Transport Association (IATA) RP 1797, Internet Engineering Task Force (IETF) related to network and electronic communication protocols as well as SO/IEC 15415 (2D Barcode) and PDF417 2D are covered as well.

Mühlbauer has more than 30 years of experience in manufacturing, delivering and installing high security solutions for ID card, passport and ePassport projects, personalization systems, travel document facilitation and verification solutions, identity management as well as eGate, Self-Service Kiosk and Automated Border Control (ABC) Solutions.

Several installations have been rolled out in the field of ABC. Selected examples are Bratislava international airport of Slovakia, Muscat international Airport in Oman, Budapest international Airport in Hungary, Tesla international Airport in Belgrade Serbia, Argentina and others.

### MB FAST GATE

Designed according to the Frontex guidelines for ABC systems, the MB FAST GATE series combines:

- latest technology for accelerate and secure border control
- support of all eMRTD's, ePassports and eID cards to allowing individuals a fully automated border-crossing in a smart and rapid way.
- modern, cost-efficient and modular design, which requires little space.

The MB FAST GATE solution significantly increases the security level and reduces the workload of the controller, such as police or security staff.

The MB FAST GATE combines modern and clear design, made of secure glass and powdered steel, to minimize feelings of enclosure or claustrophobia while ensuring optimal visibility for inspectors, with high modularity and with state-of-the-art technology, including the latest biometric sensors, document readers, verification and surveillance systems. By combining the different security features, control software, gate hardware and a control mechanism, we make sure that the gate constitutes a secure solution for all your necessary processes and needs. It helps the authorities to fight against illegal entry, immigration, crime and terrorist threats. All this is according to the Best Practice Guidelines of Frontex and regarding ICAO. If another standard than ICAO is required, this must be discussed before final pricing.

The MB FAST GATE series provide security and assurance that people can move through secure areas and around the environment faster with less interruption, which leads to higher customer satisfaction. Identification of an individual no longer depends on the human factor and the chance of errors due to minor human failure is reduced to a minimum. The solution identifies the person quickly, in a two-stage identity check system, so that the person can move faster through the secure areas than when using traditional methods.

Characterized by a highly modular hardware and software architecture, MB FAST GATES offer a vast range of possibilities. Individual elements can be easily replaced or extended according to the project needs and requirements. With its high modularity, the solution is prepared for future security levels and passenger flows and for any data protection policies. Due to the universal interfaces and a highly versatile structure, the gate can be easily integrated into any public or building environment. In the single or multi-lane configuration in one-step or two steps Gate topologies are possible.

The MB FAST GATE series allow for high-speed multi-biometric verification of individuals. ID documents can be checked electronically and optically according to completeness, validity, correctness and holder authenticity in a fully automated way. Live data can be verified against data stored in the chip and on the document, or matched with any external database, such as watchlist and blacklist, national databases, AFIS, and more. The target of the system is a fast processing of the traveler in maximum 20 seconds.

In order to increase the security level of the MB FAST GATE series, the gate can be equipped and combined with a comprehensive video surveillance system to support traveler separation and avoid climb-over or break-through attempts. Additionally, left objects can be recognized and monitored. Due to these measures, the MB FAST GATE series allows to reach high security standards.

MB FAST GATES work with swing doors that can be opened 180 degrees in total, in an angle of 90 degrees in both directions from the central position. Swing doors have many advantages compared to telescopic doors. In particular, they require a less complex technology of sensors and control mechanisms, thus reducing the complexity of the implementation.

Since the whole system is ergonomic. The Gate is free from flat surfaces, nobody can place any objects on the gate. This reduces this type of failures and the resulting alarms to a minimum.

#### Options:

The system could include a *Visual Signaling* feature that uses color-coded indicators to display the operational status of the ABC system, such as *waiting for the next passenger*, *busy*, *inoperative (maintenance mode)*, *alarm*, etc.

## 2.2 Technical Description of the eGate Solution

### 2.2.1 Basic Double Door FastGate

The MB Double Door FastGate series, designed according to the Frontex best practice technical guidelines for ABC systems, combines modern, cost-efficient design and latest technology to accelerate and secure border control. Based on a user-centric approach the Double Door FastGate supports all eMRTD, ePassports and eID card and enables individuals to perform fully automated border crossing in a smart and rapid way.

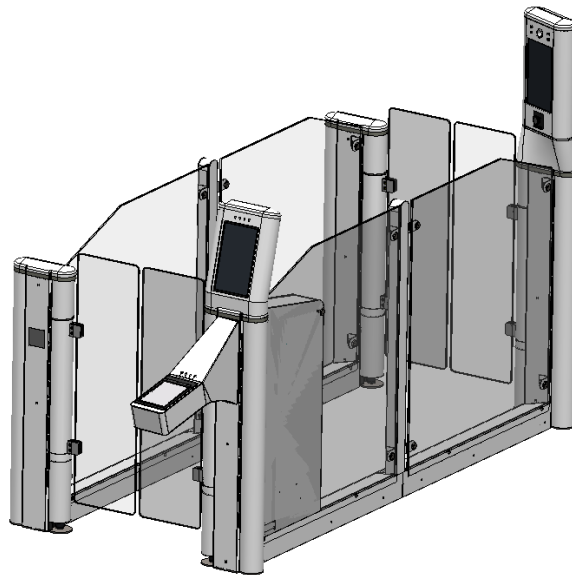
Construction of the overall Double Door FastGate is in accordance with applicable ICAO and IATA recommended practices. System is with 2 barriers (entry and exit) performing two-stage screening of the person.

The MB Double Door FastGate and its software and hardware components, are in comply with the requirements of Regulation (EU) 2016/679 (GDPR);

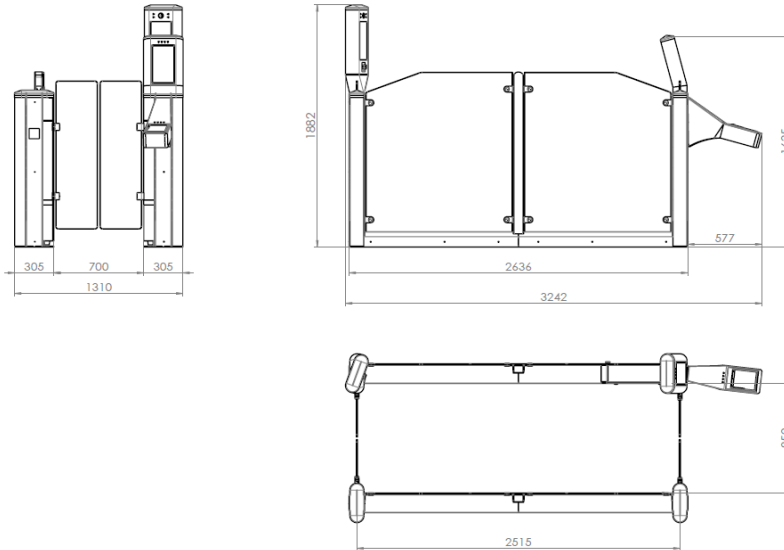
To create a secure area within geographical limits of the country, Mühlbauer provide the Double Door FastGate solution, which is the ideal system to fit in the rapidly growing market of high secure areas and automatic border crossing technologies.

The objective of the Double Door FastGate solution is a significantly increased security and a reduction of the workload of the controller, like police or security personal. In addition, in its latest generation offers the Double Door FastGate series the most flexibility, high modularity, cost-efficient design at a small space.

This system is an open design that avoids the feeling of confinement and claustrophobia and provides optimal visibility for the inspector



Proposed example of a Double Door Fast Gate

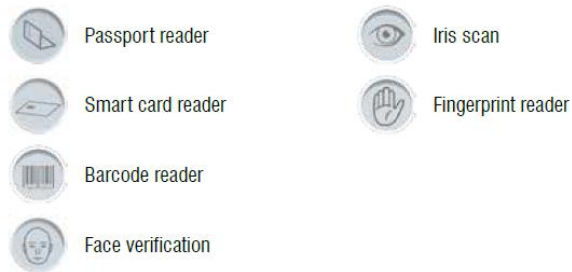


The Double Door FastGate represent a modern clear design in secure glass and powdered steel in combination with high modularity and state of the art technology, which also includes the latest biometric sensors, document reading and verification. All installed electronic and mechanical components are concealed where possible and secure;

By combining the different security features, control software, gate hardware and a control mechanism, we make sure that the gate provides a secure solution for all your necessary processes and needs. This will help the authorities to fight against illegal entry, immigration, crime and terrorist threats. All this is according to the Best Practice Guidelines of Frontex and regarding ICAO.

### FastGate components

MB Double Door FastGate can be configured with following components:



## 2.3 MB Fast Gate - Hardware

### 2.3.1 Material

- Made of Powder coating & stainless steel
- The color can be customized
- All materials used in the Double Door Fast Gate are certified for use in aviation terminals in terms of safety and health standards
- Materials used are resistant to vandalism, scratches and protected against foreign materials such as chewing gum, beverages, spilled water, cleaning fluids, etc.

### 2.3.2 UPS

#### EATON 9SX2000IR

- Output power: 1800W – 2000VA, 230VAC, sine wave, 8 x C13
- Dimensions: 608mm x 86,5mm x 438 mm,
- Weight: 26,5 kg
- Topology Online/Doublbe-conversion
- Battery: Included, Sealed, Lead-Acid, hot-swappable
- Compliances: CE marked, TUV, cULus Listed, CSA22.2, FCC part 15 Class B, CISPR22 Class B
- Cetrifications IEC/EN62040-1, UL 1778 IEC62040-2, CE, cULusListed, EAC



### 2.3.3 PC

#### GEEKOM Mini PC GT1 Mega

- Processor: Intel® Core™ Ultra 9 (185H) 14. Gen. (Meteor Lake) (16 x 1 GHz)
- RAM Memory: 32 GB DDR5-RAM 5600 MHz
- Storage: 2 TB SSD
- Graphics: Intel Arc™ Graphics
- Operating System: Windows® 11 Pro



### 2.3.4 Swing Doors

All housing parts, including the doors are easily accessible including for maintenance by an authorized person, meanwhile the panels are without sharp edges but a curve radius for higher safety. For additional injury prevention of the traveler or his luggage, the doors will be secured by security locks and levelled with said panel. Round corners also provide additional safety for travelers and make for a more aesthetic look of the Gate.

Entry Door: 1300 mm  
Exit Door: 1300 mm

- Swing doors
- With linear (rotary) motor
- Made of safety glass
- In the closed position, the doors have an opening of 50 mm
- The doors can be opened at a 90-degree angle
- The doors will not allow people moving in the wrong direction to enter the gate.

### 2.3.5 Side Walls

- Made of safety glass
- height of 150 cm
- Glass engraving on both side walls

### 2.3.6 Sensors, alarms & security

- Anti-tailgating and 2 person detection within interlocking zone
- Observes two person detection, forgotten objects, climbing over, passing under, door hit etc. The operator has the possibility to detect the complete interior zone of the gate
- The gate' sensors that are applied to prevent improper use of the gate system are combination of advance sensors technologies integrated inside the gate (no additional camera from top and sensors in handrails).
- The gate doors can detect any obstacles, which comes during doors movement in between. The integrated sensors are smart enough and prevent the travelers from any physical injuries or damage.
- The MB FastGate is equipped with integrated advance radar LIDAR sensors; the sensors can track the position of the traveler inside and outside of the gate area.
- In case of unsuccessful identity verification: the person is forced to leave the gate or stay until released by an officer.
- The attempt to force the Gate doors can be detected, if someone tries to force closed/locked doors and get it open by force then an alert to the monitor office will be sent through software.
- Ability to detect a passenger traveling in the wrong direction

### 2.3.7 Key Switch

One key hidden switch (on exit) side provides following functions:

- Turn counterclockwise unlock the far doors of the gate and set them powerless
- Turn to the middle position - activate locking mechanism and apply power

### 2.3.8 Led indicators

- Modern LED (RGB) indicators light
- On each door columns (rear & front)
- User guidance for the status of the gate e.g. ready to use (green) or not to use (red)
- LED's at Bio Devices

### 2.3.9 Modularity

- All components are easy removable and can replace in very short time are covered and not accessible from outside.
- Parts like monitors, document reader, fingerprint sensor, face camera unit etc. are replaceable in less than 30 minutes.
- Standalone gate can be expanded to multi row gate by adding gates side by side.
- The separating glass wall is reduced from resulting two walls to one shared wall.
- The resulting number of glass walls results in: Number of multi row gates + 1.

### 2.3.10 Document Reader

The Regula document reader is a proven system at Mühlbauer. The reader provides the reading of the MRZ (machine readable zone) and visual Optical Character Recognition (OCR) in accordance with ICAO 9303 (ID-1, ID-2, ID-3). It includes a visual optical character recognition for non-MRTDs and barcode recognition and reading for 1-dimension and 2-dimension bar codes. The product is certified accordingly:

- International Labor Organization (ILO) with 2D barcode parsing in seaman's documents;
- ISO 9001:2000
- CE
- RoHS
- Microsoft (for optical and RFID driver)
- BSI (EAC compliant system)

Additional licenses for verification of the optical security check like AAC and VIZ are included with regular databased updates (no additional fee).

A small-sized reader for desktop use. Hard plastic body. The device is connected to a PC via a USB cable. No moving parts. Reliable, convenient and easy-to-use. The device allows capturing images in white, infrared, ultraviolet and coaxial lights. Certain models are equipped with modules for reading RFID chips and smart cards. The device is supplied with software development kit (SDK) for easy integration into existing end-user systems. Reader Regula can be optionally equipped with a flip-top cover.

#### Functionality

- Capturing and processing images
  - supported document formats
    - ID-1
    - ID-2
    - ID-3
  - other documents with maximum size 90×130 mm
  - automatic detection of a document in a scanning zone
  - automatic scanning after document detection
  - elimination of glare from laminate and holograms in white and IR light
  - compensation of external light hitting during image capture in ultraviolet light (Smart UV)
  - automatic selection of UV illumination intensity according to the document type

- search and cropping of a document image from a general image
- The MRZ detection and recognition
- Recognition and reading of 1D and 2D barcodes from documents and screens of mobile devices
- Automatic recognition of a document type
- Processing graphic fields
- OCR of the visual zone
- Reading RFID tags
- Analyzing and comparing text data
- Automatic authenticity verification of a document

### Operation

1. The optical reader automatically detects a document in the scanning area of the device.
2. Document images are captured in different illumination modes. At the same time data is read from RFID tags and smart cards.
3. Regula Document Reader SDK processes data.
4. Results of the verification are ready for further use.

### RFID-reader

- Supported standards — ISO 14443: RFID tags of type A and B
- PC/SC protocol support
- Data exchange rate, Kbaud — 106, 212, 424, 848
- Reading an RFID tag regardless of its position in a document
- Anti-collision: reading an RFID tag according to the MRZ

### Technical specifications

- Dimensions (length×width×height), mm — 200×150×96
- Power supply voltage, V — 9...28 (12/24)
- Rated current, A, max (for 12 V) — 0,6

### Optical document reader

- Field of view, mm — 90×130: full passport page
- Sensor:
  - type — CMOS
  - colour model — RGB
  - colour depth, bit — 24

Other functionalities and details are described in following table:

#### Document image capture and processing

Document formats

- ID-1 (identity card)
- ID-2 (passport card, visa)
- ID-3 (passport)
- Other document formats up to 90 ×130 mm

Scanning process

- Document detection sensor
- Automatic scanning after document detection
- Elimination of glare from laminate and holograms for white and infrared illumination
- white and infrared illumination
- Compensation of external light hitting during image

## Machine readable zone (MRZ)

Supported MRZ formats

Features

## Barcodes

Supported formats

Authentication

## Automatic document type recognition

Order of document type  
recognition

Features

## Graphic fields processing

Types of graphic fields

Features

- Capture in UV light (Smart UV)
- Automatic intensity selection of UV illumination for a certain document type
- Search and cropping of a document image from a received image
- In conformity with ICAO 9303:
  - 44×2
  - 30×3
  - 36×2
- In conformity with ISO IEC 18013 (IDL):
  - 30×1
- Support of special MRZ data structure for documents of certain countries
- Search for the MRZ along the whole document image
- MRZ recognition in infrared and white light
- Control of check digits and data structure in conformity with the requirements of ICAO 9303 and BSI TR-03105 Part 5.1
- Evaluation of MRZ quality specifications in conformity with ICAO 9303, ISO 7501, 1831, 1073-2 standards
- 1D: Codabar, Code39 (+extended), Code93, Code128, EAN-8, EAN-13, IATA 2 of 5 (Airline), Interleaved 2 of 5 (ITF), Matrix 2 of 5, STF (Industrial), UPC-A, UPC-E
- 2D: PDF417, Aztec Code, QR Code, Datamatrix
- Barcode format check
- Country→Type→Series
- Receiving a document template from the SDK database containing the following information:
  - Text and graphic fields position
  - Availability of barcodes and security features
  - Authenticity verification and its parameters
  - RFID-chip availability
  - A reference image from Information Reference Systems «[Passport](#)», «[Autodocs](#)», «[Frontline Documents System](#)»
  - Processing of the received document images in compliance with the sample, including document image rotation by the angle given in the sample
- Portrait of the document holder
- Signature
- Barcode
- Fingerprint, etc.
- Cropping and displaying graphic fields as separate images in compliance with the sample of the corresponding document

### OCR of the visual zone

Recognition of character sets

Features

### RFID SDK

Supported RFID-chip  
Standards

Data access modes

Authentication

Supported applications

Certificate management

Features

### Analysis and comparison of text data

Document areas for cross-checking of the  
readout data

- Automatic searching of faces on the document image and cropping the document holder portrait if the document type is not recognized
- Document image rotation according to the document holder portrait position
- Central European and Eastern European Latin (1250)
- Cyrillic (1251)
- Western European Latin (1252)
- Greek (1253)
- Turkish (1254)
- Baltic (1257)
- Other fonts of any size
- Dictionary support (name, surname, address, country, etc.)
- Automatic text division into separate fields (e.g. dividing the address into postal code, country, state, etc.)
- Recognition of dates with complex formats
- Recognition of characters from different character sets in one line
- ISO/IEC 14443-2 (type A and B)
- ISO/IEC 14443-3 (MIFARE® Classic Protocol)
- ISO/IEC 14443-4
- Direct
- BAC
- EAC
- PACE
- SAC
- Active (AA)
- Passive (PA)
- Chip (CA v1, CA v2)
- Terminal (TA v1, TA v2)
- ePassport (DG1–DG16)
- eID (DG1–DG21)
- eSign
- eDL (DG1–DG14)
- Local storage
- Receiving certificates online through the program interface
- Master List, CRL support
- Reading RFID chips with extended length support
- Reading RFID chips in compliance with ICAO LDS 1.7, PKI 1.1 data formats
- Certified by BSI TR-03105 Part 5.1, BSI TR-03105 Part 5.2
- MRZ
- VIZ
- RFID-chip
- Barcode

## Verification

Adjustment of formats and measuring units to those used in the user OS

## Features

### Authenticity verification

Operation available for any document

Operations available after document type recognition

### Additional SDK functions

Image formats

Interoperability

OS compatibility

- Validity of any dates
- Authenticity of names and surnames according to lists of wordstops
- Zero numbers of sample documents
- Date
- Weight
- Height, etc.
- Complete or partial comparison of fields
- Integration of data received from several document pages
- Calculated field support (age, etc.)
- Transliteration to Latin characters in compliance with ICAO 9303 standards for comparison with the MRZ
- Checking luminescence (UV Dull Paper) of:
  - Form
  - MRZ area
  - Portrait area
- Checking the MRZ print contrast in compliance with ICAO 9303(IR B900 Ink)
- Checking image patterns in white, IR and UV light
- Checking luminescence of UV protection fibers
- Detection of false luminescence
- Checking photo embedding type: printing or attachment
- Checking IR Visibility of:
  - Elements of the form
  - Text data
  - Photograph (main and additional)
- Detection of holograms (OVD), OVI
- Reading a luminescent text and comparing it with the data obtained from the MRZ and VIZ (OCR Security Text)
- Visualization of IPI (Invisible Personal Information)
- Checking retroreflective protection
- Checking barcode format
- \*.BMP
- \*.JPG
- \*.JP2
- \*.PNG
- \*.TIF
- other image formats are possible on request
- Comparison modules:
  - Fingerprint images from RFID chip and external fingerprint scanner
  - Face images from document data page and/or RFID chip
- Information Reference Systems «[Passport](#)», «[Autodocs](#)», «[Frontline Documents System](#)»
- Windows 7 (x86, x64), Windows 8, Windows 10

Drivers  
Features

**Software updates**

SDK

**Document template database**

**Functionality**

Optical Reader Light Sources

Reader of radio frequency  
identification devices (RFID)

Number of megapixels

Resolution, ppi

Frame size, pixels

- Microsoft certified
- Simultaneous optical scanning and RFID chip reading
- Firmware upgrade via USB interface (automatic upgrade after installing new SDK version)
- Multilingual interface
  
- Twice a year
- Monthly
  
- White
- Infrared 870 nm
- Ultraviolet 365 nm
- Coaxial White
- Included
  
- 5 MPx
- 460 +/- 3%
- 2592x1944

Note: In case not all the features are listed, please note that the document reader will meet the criteria of Annex 2.

### 2.3.11 Dual Interface Smartcard Reader

HID OMNIKEY 5422

- Supporting T=0, T=1, ISO7816 Class A/B/C
- USB 2.0 (USB 3.0 ready)
- Windows 10
- Switch between C & CL



### 2.3.12 Biometric face camera

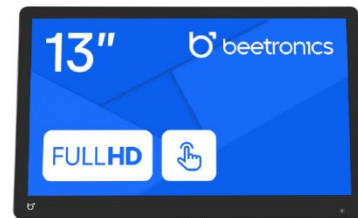
- Mühlbauer uses a wide-angle camera for face recognition.
- This camera detects the traveler's face and height between 1.100 mm and 2.200 mm. The camera also detects the traveler's face on a distance between 60 cm and 140 cm.
- A display integrated in Face recognition unit for user guidance and instructs the face verification process to travelers e.g. verification successful or failed etc.
- In order to capture high quality images face recognition unit has bright and diffuse illumination.
- Depending on the requirement, the face detection range for height and distance could be customized.

Face Verification licenses are included



### 2.3.13 Monitor/Display

- 13.3"
- Full HD
- Touch technology – capacity
- Edge to edge glass
- Anti-fingerprint coating
- Representation of the travel documents on document scanner
- The small monitor shows all instructions for actions such as, placing the document, reading and processing in simple, clear form and independent from language. The monitor shows how the travel document must be read by the reader by using animations and graphic, so that it can be properly read. After the user has placed the document on the reading unit of the device as shown on the monitor, the device starts reading the ePassport/card data, which is illustrated by an animation on the screen like
- Mistakes errors can be detected during this phase of the process, e.g. not presenting the holder page of the passport. Such errors will signal to the traveler to correct his mistake or he will be directed to a manual control
- As soon as the process of reading and verifying data is successfully completed and the document is no longer on the reader, the exit door opens automatically. At the same time both lamps change from red to green, giving the passenger the signal to move further.
- In case the document is not compliant, etc. the same pictograms as shown above direct the traveler to manual inspection
- If the passenger leaves his passport on the document reader, then the eGate will issue an optical and acoustic alarm after a certain



amount of time, requesting the passenger to remove the document from the reader.

- However, should the reading the verifying process not be successful, the exit symbol in the gate area remains red and the user is shown on the monitor to move to manual passport control

### 2.3.14 CCTV

- FastGate installed area can be observed through additional CCTV camera.
- A dome camera is installed on top of each eGate in order to allow full surveillance of the persons passing and activities inside the eGate.
- Each camera is a HD 2 MPixel IP PoE color video camera, which is connected to a network.
- The cameras work under ambient light conditions
- Network Video Recorder (NVR) system with capability to store video surveillance footage from each camera at the eGate in digital format to hard drives up to 30 days.



### 2.3.15 Installation

- Solid floor
- Anchor bolts (provided with the gate); options – glue, cabling from top and podium
- Floor load capacity: min. 200kg/m<sup>2</sup>

### 2.3.16 SDK for Bio Devices and Gate Control

Mühlbauer will provide latest SDK from supplier of the following devices:

- Face Camera
- Document reader

also with documentation related to that SDK.

SDK for Gate Control:

The SDK package includes a Windows DLL to control the gate hardware (doors, sensors ...) and a Windows DLL for Vision software. Furthermore, a test application to check the gate hardware will be provided.

Note:

The SDK for the Bio devices are included in the Fastgate.

Iris Camera is not part of SDK; it is provided a API from the manufacturer of the camera. The detailed specification of the SDK was submitted in a separate document.

## 2.4 MB Fast Gate – Software / Control and Monitoring of the ABC System

This proposal has been developed to supply, Installation and Commissioning of ABC Gates at Chisinau airport. The eGate is design based on state-of-the-art technology fully capable of scanning and verifying electronic document (e.g. ePassport, eID etc.) against respective template, reading chip information, performing various biometric verification including facial and fingerprint verification as well as tailgating detection and prevention. In order to complement the eGate it is also supported by software components like Border Guard Control Unit, Terminal Control Center and User Management.

Border Guard Control Unit is the module that allows border police to manage and monitor the eGate. Its instance is running on the server located within server room at Bandaranaike International Airport and accessible via browser. It allows border police to perform various operations including initiation, activation and monitoring current process happening at the eGate remotely.

Border Management Adapter's function is to serve as interface between Mühlbauer software components with external system including border management system via encrypted communication channel using REST API. It can also be connected to stop-list system and others. Existing system owner needs to provide complete technical specification, data format and other related information for each system to be integrated with proposed automated border control system. Full support from client is required in order to ensure the integration process is seamless and successful.

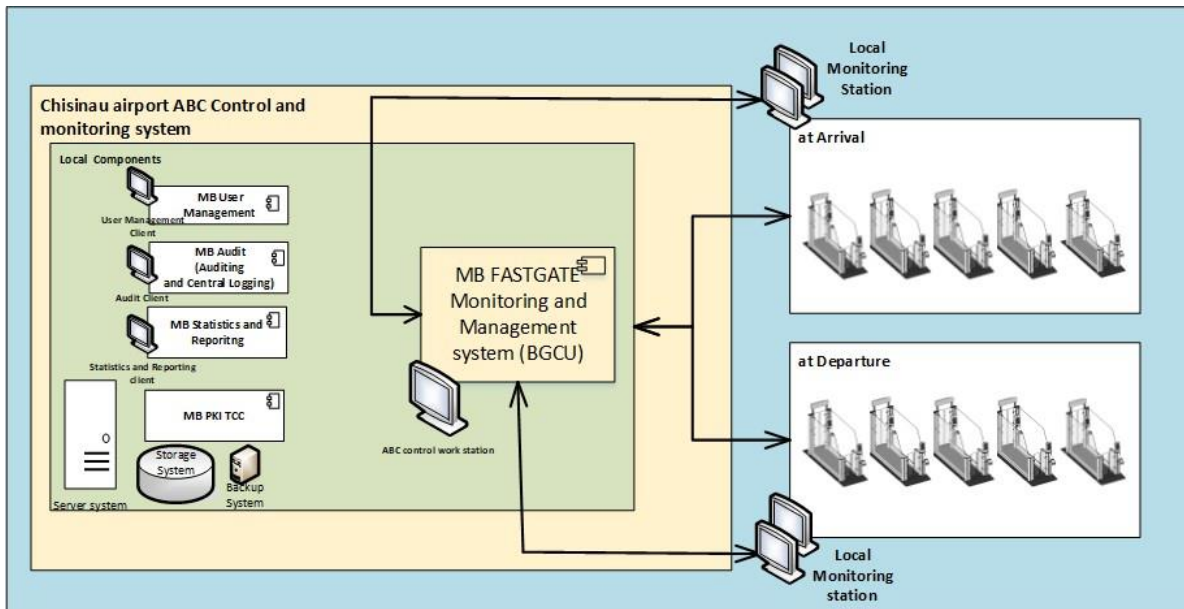
User Management software allows administrator to manage and monitor personnel and assign access to related systems accordingly.

All eGate, servers and workstations will be setup at location specified by client and connected to local network using Ethernet connection.

The proposed solution ensures system resilience against potential threats while adhering to recognized best practices for secure architecture, thereby enhancing operational reliability and compliance with industry standards

The delivery of this project includes

- Automated Border Control eGate in technical specification document. Mandatory components include
  - Double door
  - Document reader
  - Facial verification camera
  - Fingerprint scanner
  - Display/Monitor unit
- Software components
  - Border Guard Control Unit (BGCU)
  - Border Management Adapter (BMA)
  - User Management (UM)
- Hardware components
  - Virtualization and Management Servers (including rack)
  - Network components (switch, firewall etc.)
  - Client workstation for BGCU and Administrator



Graphical representation of solution implantation (exemplary)

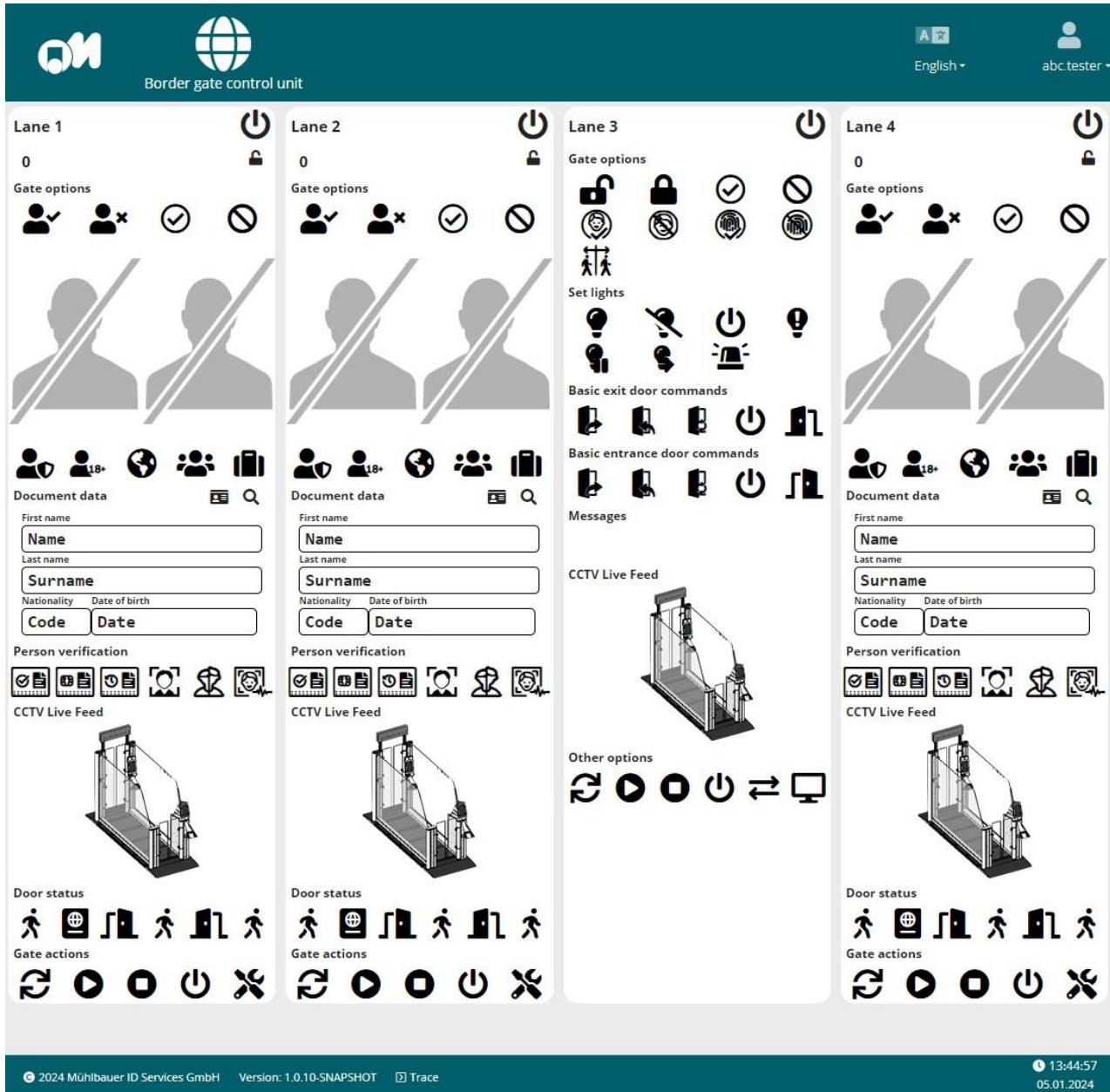
### 2.4.1 Border Guard Control Unit (MB BGCU)

The MB eGates are delivered with the management module for the border police to monitor and control the eGate and kiosk. This software module is called Border Guard Control Unit (BGCU) and runs on a dedicated management workstation. The management workstations are

- For monitoring individual MB eGate systems
- Allow for remote control in the scope
  - initiation of gate systems
  - enable the activation
  - display individual process stages during the border check

Two monitoring workstations are suited for monitoring and controlling up to five devices represented by MB eGate. A separate section on the monitor is provided for every connected MB eGate. The number of displayed devices can be configured. Only authorized personnel (managed via User Management system) is allowed access to this system.

Through the Monitoring Station, the inspector have full control of the ABC System and it is able to open both entry and exit doors (the door will close automatically when time expires or after the passenger has passed), reset/restart and activate/deactivate the MB eGates.



Picture of BGCU – Monitoring Client (exemplary)

In the above exemplary image, all the lanes are functional except lane 3. Lane 3 is the service view of the eGate where the operator can open the doors, lock or unlock the gates and so on. Every single gate has this option.

The display and control section of the monitoring workstation graphic surface is divided into the following categories:

- Displaying the overall result of the border control process by using a color indicator. After document has been read, fields that can be validated from document turn green or red, depending on validation result. When passenger enters inside gate biometric verification and watch-list result change color to green or red, depending on result. Retrieved information including biometric information and verification result will not be saved locally but sent (via web interface) to intended system specified by client.
- Indicating range for status information and testing errors
  - Functional status of the device
  - Display if the facial verification timeout has been exceeded

- Visualization of the results of the facial recognition procedure is displayed when it falls below the specified minimum value.
- Visualization of live video image from the integrated facial camera of the ABC system.
- Display, if the emergency off switch has been activated in the gate
- Automatic alarm function
- The person can be released with a physical key switch or virtual switch displayed in the boarder control software GUI
- Indicating range for document authentication and biometric verification:
  - Watchlist request result
  - Document authentication result (shown separated into visual-physical and electronic examination)
  - Biometric verification result including the matching score
  - Display of the image read off the chip and the recorder live image. Optionally, the section can also show the facial image from the optical scan extracted from the holder page.
  - Display of extracted personal and document data. Among others, document type, country, name, date of birth, validity, etc.
- If the surveillance has registered more than one person:
  - An attempt of circumventing
  - Objects left behind
  - Indicating range for security camera signals
- Control section for MB eGate remote control. The most important buttons are displayed directly and are for base functions that are executed quickly such as opening the exit door or locking both doors. Further control functions can also be executed by monitoring workstation. Real time monitoring is possible of the border crossing process by the offered control and monitoring work stations. To do that, a service sub-menu can be displayed for every gate system. This menu provides functions such as activation or deactivation of a gate system.

Offered BGCU system ensures the integration with the airport ecosystem (including DCS, AODB, FIDS, and RMS).for efficient operation. It is assumed that the interface specification of the existing system will be provided for the integration. The BGCU system offers webservice interface (REST / SOAP) for receiving data and for returning feedback information from ABC system.

Overall processing time is impacted by several factors, including the type and complexity of the travel document, passenger behavior and cooperation during processing, and the response time of the IGPF SOAP-based service. Notwithstanding these variables, the proposed solution has been specifically engineered and optimized to meet defined performance requirements in the vast majority of cases, ensuring efficient, reliable, and consistent operation under typical usage conditions.

The MB eGates have an emergency switch/button that allows the passenger to request assistance from the inspector. The emergency switch is triggering an alarm but its not automatically release the barriers. The inspector is able to open the entry barrier using an 'emergency button', which shall not accessible to the passenger at the second stage of the check;

The offered system offers backup plans in case of external systems unavailable by including retrying failed requests, queuing data to be sent later, using cached or backup data and sending alert to infrastructure systems. However, the backup plans is also interface specification provided.

The BGCU application program interface (API) is designed to seamlessly integrate with the airport's external systems, contingent upon the provision of the relevant interface specifications by the governing authority.

### 2.4.2 Passenger passes process

The standard passage process consists of two main phases:

- Document Readout & Pre-Gate Evaluation
  - The system reads and verifies the passenger's travel document before entry.
- In-Gate Verification & Clearance
  - The system assesses tailgating, biometric authentication, and checks against law enforcement databases while the passenger is inside the gate.

Successful passes - upon arrival at the gate, the passenger presents their travel document to the reader, which captures and processes all necessary data. A comprehensive verification is then conducted, for example image pattern recognition, passive authentication and chip authentication.

If all security and validation checks return positive results, the entry doors open, allowing the passenger to proceed. Once inside, the entry doors close, initiating parallel evaluations for tailgating detection, automatic facial recognition (including facial comparison between the document chip and gate-captured images, as well as liveness detection), and clearance against police databases.

Provided no tailgating alerts are triggered, biometric authentication is successfully completed, and the passenger is not listed in any law enforcement watchlists, the exit doors open, enabling the passenger to leave the gate. Once the passenger exits and the doors close, the system resets, becoming fully operational for the next traveler.

Unsuccessful passes - upon arrival at the gate, the passenger presents their travel document to the reader, which captures and processes all required data. The system conducts a full verification, for example image pattern recognition, passive authentication and chip authentication.

If all security and validation checks are passed, the entry doors open, allowing the passenger to enter. Once inside, the entry doors close, triggering parallel evaluations for tailgating detection, biometric verification, and clearance against police databases.

In cases where tailgating is not detected and the passenger is not listed in law enforcement watchlists, but biometric authentication returns a negative result, the system alerts an operator for manual review. If the operator determines— based on photo comparison—that the discrepancy is due to an outdated passport photo rather than identity fraud, the passenger may be manually approved via the BGCU system. Upon confirmation, the exit doors open, allowing the passenger to proceed. Once the passenger exits and the doors close, the system resets for the next travel.

The supplier shall provide full documentation on the API structure used by the ABC System (methods, parameters, responses, error codes, authentication);

### 2.4.3 Border Management Adapter (MB BMA)

The MB BMA Software serves multiple functions. Its main function is to serve as a link between Mühlbauer software components with external system including border management system. MB BMA creates a secure communication channel encrypted via REST API protected by TLS 1.3 standard. It provides API for standard data elements exchange. It is also very flexible so it can be adapted to connect to 3rd party APIs. This means the component is designed to exchange data with stop-list system. It also has the functionality to verify the data obtained by the MB eGate system against the National Border Control System or other external system.

In alignment with the published API specifications provided by the IGPf, ABC System will develop and implement the requisite services to ensure seamless integration and interoperability with external systems. Our solution will fully support SOAP-based web service protocols, enabling standardized, secure, and reliable communication channels.

These services will be architected following best practices to guarantee high availability, scalability, and compliance with industry standards, thereby facilitating smooth data exchange and operational consistency across platforms.

By leveraging SOAP protocol, ABC System will ensure robust message formatting, comprehensive error handling, and support for WS-Security features, thus meeting the stringent requirements of enterprise-level integrations as outlined by IGPF.

We can also provide full documentation on the API structure used by the ABC System (methods, parameters, responses, error codes, authentication). To ensure that the API meets all relevant functional safety requirements, the following test methods is applied in accordance with applicable standards.

- Unit Testing
  - Verification of individual API components/modules in isolation to ensure correct functionality before integration.
  - Test cases will include normal operation, boundary conditions, and error-handling paths.
  - Automated unit test frameworks will be used to ensure repeatability and traceability to safety requirements.

#### **2.4.4 MB Trust Inspection System**

Terminal Control Centre (TCC) is an advanced supplementary service to the PKIs supporting Electronic Passports and the cornerstone to an effective full automation of border control.

MB's TCC solution (mTCC) centralizes lifecycle management of keys and X.509 and CVC certificates needed by Inspection Systems on Automated Border Control gates, enabling terminals to read and validate electronic travel documents and make use of advanced authentication mechanisms such as biometrics.

Besides managing keys and certificates, mTCC proxies nPKD to the Inspection Systems, making available all the required information for correct and complete validation of electronic travel documents.

NOTE: nPKD is not offered in this solution.

#### **2.4.5 MB User Management**

Information is an important value to government agencies, and must therefore be appropriately protected. This information is mostly collected, processed, used and transmitted in electronic form. The business process also has to provide that the data is processed confidentially and the data is available for the needs of the business process.

IT security must be ensured in order to protect the information and the applications, which are needed for a business process with a sufficient level of security for the following aspects:

- Secrecy (confidentiality)
- Correctness (integrity)
- Availability

This means protecting information and information systems from unauthorized access, disclosure, disruption, modification, recording and destruction and maximizing the availability of the information for people who need it in the specific business process.

Mühlbauer User Management (UM) supports the main procedures of system security:

- User and policy management
  - Rights Management
  - Role concept

- Certificate & Key Management
- 1-factor authentication of users and applications
- 2 factor authentication of users
- Secure communication
  - Encryption
  - Signing

The offered User Management is offered with two-factor authentication for limited user. The user authentication system is capable to register less than or equal to 20 users.

#### **2.4.6 MB Audit**

Mühlbauer provides a dedicated Data Management solution, which centrally tracks actions performed inside the offered solution. This includes user actions and eGate results. The solution provides the functionality to collect and store the necessary status information and prepare them for audit lookup, report printing, statistical analysis or monitoring of current state.

MB Audit client is designed for accessing these data in an easy and user-friendly way. The information can be either sent by each Mühlbauer software component or gathered by an import-module. The web-based interface can be operated from a normal PC with a web browser.

All information processes (applications) within the ABC System will retain audit and recording data for every action executed during the border control crossing process. This data, stored locally on the ABC System processor disk in file format, will be maintained for a maximum period of seven (7) days, in alignment with operational and data retention requirements.

All system logs are retained for at least 30 days in line with applicable data protection and retention policies. These logs capture records of passenger processing activities, including all associated images. Data storage and handling is in compliance with relevant regulations, ensuring confidentiality, integrity, and controlled access throughout the data lifecycle. Configurable secure deletion processes are implemented in accordance with the Beneficiary's internal policies and the requirements of the GDPR.

#### **2.4.7 Liveness Detection System**

In order to be protected against spoofing attack, our facial and finger print verification also equipped with liveness and presentation attack detection (PAD) engine. In the offered liveness detection component and the PAD system is assured by iBeta testing with specific method and technology according to ISO/IEC 30107- 3 and follow the fundamental foundational framework according to ISO/IEC 30107- 1.

A conventional face identification system can be tricked by placing a photo in front of the camera. Same also can be happened by placing fake finger print. The proposed BGCU system along with PAD system is able to prevent this kind of security breach by determining whether a face in a video stream or single frame is "live" or a photograph. The liveness detection can be performed in passive mode.

The primarily used of the offered license is for automated border control gates (e-Gates) operation. The solution is scalable for future e-Gate expansions.

## 2.5 Deliverables for ABC e-gates HW & SW

Pos.	Description	Quantity	Comments
1	<b>MB eGates:</b> <ul style="list-style-type: none"> <li>• Document Reader</li> <li>• Face Camera with Face Liveness Detection</li> <li>• Fingerprint Scanner</li> <li>• CCTV</li> <li>• Facial Verification</li> </ul>	10	
2	<b>Software License:</b> <ul style="list-style-type: none"> <li>• 1x Border Guard Control Unit software license</li> <li>• 1x Border Management Adapter software License (API)</li> <li>• 2x Terminal Control Center software license</li> <li>• 1x User Management Software License</li> <li>• 1x Audit software</li> <li>• NEUROtechnology liveness detection image technology</li> </ul>	1	
3	<b>ITC Hardware:</b> <p><b>Storage</b></p> <ul style="list-style-type: none"> <li>• 1x Storage</li> </ul> <p>General details:</p> <ul style="list-style-type: none"> <li>○ 25 TB usable space</li> <li>○ 4x 16 Gb FC</li> </ul> <p><b>Virtualization Servers</b></p> <ul style="list-style-type: none"> <li>• 2x Virtualization servers</li> </ul> <p>General details:</p> <ul style="list-style-type: none"> <li>○ 2x AMD EPYC 9124 3.0GHz</li> <li>○ 8x 32 GB RDIMM, 5600MT/s</li> <li>○ 1x Boss card 960 GB</li> <li>○ 1x Virtualization licenses included</li> <li>○ 8x SO Windows server 2025</li> </ul> <p><b>Management Server</b></p> <ul style="list-style-type: none"> <li>• 1x MGMT Server</li> </ul> <p>General details:</p> <ul style="list-style-type: none"> <li>○ 1x AMD EPYC 9124 3.0GHz</li> <li>○ 2x 32 GB RDIMM, 5600MT/s</li> <li>○ 1x Boss card 960 GB</li> </ul> <p><b>Hardware Dongle Server</b></p> <ul style="list-style-type: none"> <li>• 1x Hardware Dongle Server for 20 ports</li> </ul> <p><b>Network</b></p> <ul style="list-style-type: none"> <li>• 2x Switches, 24 PoE ports, + 4 SFP</li> <li>• 1x Switch, 24 ports, + 4 SFP</li> </ul> <p><b>Firewall</b></p> <ul style="list-style-type: none"> <li>• 2x Firewalls, 22 ports, 2x 10 GE SFP+, 4x SFP</li> </ul>	1	

	<p><b>Antivirus</b></p> <ul style="list-style-type: none"> <li>• Licenses for 30 devices included</li> </ul> <p><b>Backup &amp; Recovery</b></p> <ul style="list-style-type: none"> <li>• Backup Tape Library including cartridges for 180 TB</li> <li>• Backup license for 20 machines</li> </ul> <p><b>Rack, KVM, UPS</b></p> <ul style="list-style-type: none"> <li>• 1x 42U Rack-Mount</li> <li>• 1x UPS 5000VA, 1x EBM for 180V</li> <li>• 1x KVM Console Switch, 4x Combo kit cables</li> </ul> <p><b>All-in-One PCs</b></p> <ul style="list-style-type: none"> <li>• 6x All-in-One PCs</li> </ul> <p>General details:</p> <ul style="list-style-type: none"> <li>○ 24" Monitor</li> <li>○ Intel(R) Core(TM) i5-14500T</li> <li>○ 16 GB RAM</li> <li>○ 256 GB SSD</li> <li>○ Windows 11 Pro</li> <li>○ Keyboard + mouse</li> <li>○ UPS</li> </ul> <p><b>Display 65", 32"</b></p> <ul style="list-style-type: none"> <li>• 2x 65" Displays</li> <li>• 10x 32" Monitors</li> </ul> <p><b>HSM Security Server</b></p> <ul style="list-style-type: none"> <li>• 2x HSM Protect Server + Toolkit</li> </ul>			
--	--	--	--	--

## 3 Services for ABC e-Gates

### 3.1.1 Project Initiation

A Kick-Off meeting between the supplier and customer prior to any project execution is integral to the project's success. During these meetings, a common language is developed, goals are set and important discussions on expectations are held. Without this meeting, the project is vulnerable to ambiguity, miscommunication and other risks of any kind.

Provider's team is meeting remotely with Customer to clarify (among others) the following topics:

- Project goals / scope of work / deliverables / expected outcomes
- Project team
- Responsibilities (supplier & State border police )
- Project schedule and milestones
- Key success factors / dependencies / risks
- Delivery and acceptance
- System / software specification
- Guidelines

### 3.1.2 Pre-Commissioning at the supplier Facility (Mühlbauer)

For the preparation for the Factory Acceptance Test of the proposed equipment and software solution, Mühlbauer will pre-install the equipment & at its systems. The pre-installed systems will be configured to demonstrate the functionality of the solution at Mühlbauer facility in Roding, Germany.

Please note that central/client system software components will be installed on test equipment

### 3.1.3 Training for customer at Mühlbauer Facility

Provider offers training services tailored to the individual requirements of the project through a customized training plan for each training level.

In order to train technical team of customer nominated to perform basic maintenance activities of the equipment & software at Chisinau Airport site, provider offers following training courses in Roding, Germany to customer team:

- Solution Overview & Solution Operation (1 day)
- Basic Maintenance & Troubleshooting (1 day)

### 3.1.4 Factory Acceptance Test (FAT)

A Factory Acceptance Test (FAT) is a major project milestone and attended by provider, Customer or a suitable representative.

During the FAT, Mühlbauer tests the Equipment and Systems according to customer-approved test plans and specifications to demonstrate that it meets the customer's requirements.

During the FAT, the test team shall:

- Verify the completeness of the deliverables (bill of materials).
- Review the specification while checking the Equipment and Systems for its compliance with it, including the Equipment safety concept.
- Test the Equipment and Systems with the procedure that has already been approved by Mühlbauer and the Customer. Included shall be functionality testing and regulatory testing.
- Note the software versions installed in the Equipment that is being tested.

After the solution has passed the test procedure, the shipment will be performed.

### **3.1.5 Logistics**

Logistics will be done according to the tender requirements.

### **3.1.6 Installation and commissioning at Chisinau Airport, Moldova**

Installation and Commissioning is a key part of putting e-Gate solution into operation.

The Installation and Commissioning of the e-Gate solution is performed by a team of experienced engineers and comprises typically the following activities:

- Unpacking and Positioning of the Equipment to the final site
- Equipment Installation - the physical installation of the Equipment and the Systems at the customer's facility, including the connection to the necessary infrastructure, such as power supply, communication networks etc.
- Commissioning – e-Gate solution are powered up and tested in a standalone environment. Integration into customer environment. Test the e-Gate solution with the procedure & workflows that has already been approved and agreed during the Project Initiation.

The main objective of commissioning is to ensure the safe and orderly handover of e-Gate solution from the manufacturer to the customer and to guarantee its operability in terms of performance, reliability, and safety and information traceability.

Note: Customer is responsible to deliver provided equipment from their warehouse to the place of installation.

#### **3.1.6.1 Customer testing and validation**

Customer will be given time for further testing and validation

#### **3.1.7 Training for customer at Customer Facility**

In order to train technical team of customer nominated to perform basic maintenance activities of the equipment & software at Chisinau Airport site, provider will train nominated staff at airport for:

- Solution Operation (1 day for Entry / 1 day for Exit)
- Maintenance & Troubleshooting (1 day for Entry / 1 day for Exit)
- Solution Administration (2 days )

#### **3.1.8 Site Acceptance Test (SAT)**

Once the Equipment and Systems are commissioned and their correct operation has been tested and confirmed, the Commissioning process is considered complete and the solution is formally handed over to the customer.

In practice, the on-site acceptance process includes inspection and testing of every operational component of the Equipment and Systems, from individual functions to complex interactions including the final product of manufacturing or personalization processes.

Prior to the execution of the acceptance testing, a test plan and schedule is provided to the customer for approval.

The acceptance of the system will be recorded within a Site Acceptance Protocol, which is signed by the authorized representatives of the customer and Mühlbauer.

#### **3.1.9 Ramp-up Support**

The most critical phase of a project is the ramp-up phase, when the Solution goes live. Under supervision and with the quick response of provider's experienced engineers, the ramp-up is successfully and smoothly put into practice.

##### **Ramp-Up Support covers:**

Experienced service engineers on-site to help the customer's operation ramp-up run smoothly

Further training of operators and engineers in daily operations

Identification of improvement opportunities throughout constant monitoring and reporting

Ramp up support will start right after SAT and will be provided for two weeks

- Service Engineer located in the airport
- Mon.-Fri., 8 hours per day

## 3.2 Maintenance and Support Services

This phase is providing comprehensive and customizable maintenance and support services, which considerably contribute to a higher over-the-years economic utilization of the supported systems. The related services will be provided by a team of trained and skilled technicians who are experienced in maintenance activities such as detection, isolation and resolution of technical incidents services for your existing Personalization machines. The supplier maintenance and support concept can be summarized as below:

### 3.2.1 Corrective Maintenance

Four-level corrective maintenance is offer in order to cover Maintenance & Support Phase; Corrective maintenance consists of:

- 1st Level Support: Technical Support Group (TSG)
- 2nd Level Support Specialist Support Group (SSG)
- 3rd Level Support Research and Development (R&D)
- Field Service Support

#### 3.2.1.1 1st Level Support: Technical Support Group (TSG)

The first instance of the Remote Support, is 1st Level Support team, the Technical Support Group (TSG). Embedded in the Central Service Organization, the TSG takes care of the internal coordination for further support. The 1st Level Support is provided remote via phone and email.

#### 3.2.1.2 2nd Level Support (Remote Support)

If 1<sup>st</sup> Level Support Team is not able to solve the incident, it is escalated to the 2<sup>nd</sup> Level Support team. The 2<sup>nd</sup> level takes care of the internal coordination for further support. The relevant internal departments are involved in order to provide clarification to the inquirer via phone/ email or remote desktop support.

#### 3.2.1.3 3rd Level Support (Remote Support)

If the 2<sup>nd</sup> Level Support efforts could not solve the incident, it is escalated to the 3<sup>rd</sup> Level Support team, the Software Development or R&D teams. The relevant internal departments are involved in order to provide clarification to the inquirer via phone/ email or remote desktop support.

#### 3.2.1.4 Field Service Support

The Field Service Support is provided by local qualified service engineers. Corrective Maintenance tasks for incidents which couldn't be resolved by the means of the central support levels are forwarded to the Field Service. Depending on the nature of the incident, local service engineer is then dispatched in close consultation with the customer.

## 3.2.2 Preventive Maintenance

Preventive Maintenance is the systematic care and protection of Equipment and Systems in order to keep them in a safe, usable condition that limits downtime and extends productivity. Damage to the Equipment and Systems might be easy to repair, but can cause high effort and costs if detected too late.

### 3.2.2.1 Preventive Maintenance for eGates

Preventive Maintenance includes the following tasks:

- Early detection of damage and wear, minimizing the risk of unplanned Equipment downtime;
- Exchange of information between engineers;
- General check of Equipment's software and hardware;
- Sensor and actuator tests including adjustment, if necessary;

- Inspection of all moving parts, pin joints, guides, etc. including adjustment, if required
- Refresher training of maintenance personnel to perform daily maintenance;

Once per year 1x Hardware Service Engineer for 4 working days ( 2 days for entry & 2 days for exit ) conducted on site

### **3.2.2.2 Remote Preventive Maintenance for eGates Software Components**

Preventive Maintenance is the systematic care and protection of Equipment and Systems in order to keep them in a safe, usable condition that limits downtime and extends productivity. Damage to the Equipment and Systems might be easy to repair, but can cause high effort and costs if detected too late.

We recommend regular remote Preventive Maintenance by service engineer periodically to keep the production in top condition. Preventive Maintenance of following will be provided once per year:

- Software Solution ( remotely ) during 3 days
- Remote connection ( If applicable ) has to be arranged by customer

### **3.2.3 Software Subscriptions**

Required yearly software license or maintenance fees or subscriptions are included in this offer.

Besides the software support, the Software Maintenance Basic contains the following services:

- Correct function of the system software (Bug fixing)
- Software updates (Excluding change request and any 3<sup>rd</sup> party licenses)
- Security patches for operating systems if applicable

Please note before applying software updates respective backups are taken to make sure restore point in case of malfunction caused by update.

### **3.2.4 Warranty - Supply of Spare Parts**

Supplier warrants our Systems and Equipment are free from defects in material and workmanship upon delivery, subject to normal use and under normal environmental and maintenance conditions. Supplier offers all new Systems and Equipment with a standard warranty as required in the tender and a guarantee of availability of spare parts as required in tender from the date of Site Acceptance Test.