RSD
RELIABLE SOLUTIONS DISTRIBUTOR

Mühlbauer
High Tech International

Mühlbauer ID Services GmbH

Tender No. 21590534 (ocds-b3wdp1-MD-1774963944764)

Automated Border Control System (Automated Border Control, ABC, eGate)

Digitally signed by Bîrsan Vitalie
Date: 2026.05.06 13:11:21 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Technical Description

Associated Tenderers

Lead: I.C.S. "Reliable Solutions Distributor" S.R.L.
85 Alexandru cel Bun st.
Chișinău MD-2012.
Republic of Moldova

Associate: Mühlbauer ID Services GmbH
Josef-Mühlbauer-Platz 1
93426 Roding
Germany

Table of Contents

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

Requirement	Compliancy
The ABC system must provide travelers with a fully automated border control process, with self-service capabilities, performing comprehensive checks of travel documents and biometric facial identification of passengers, in accordance with the Frontex Agency's "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems."	
1. General requirements for the ABC System	
1.1. The design of the general ABC System must comply with applicable ICAO and IATA recommended practices;	**Compliant** Please ref. to chapter 2.2.1
1.2. The ABC System must be designed with two barriers/gates (entry and exit) to perform two-stage passenger screening. Each stage must include a double Gate barrier;	**Compliant** Please ref. to chapter 2.2.1
1.3. The design of the ABC System must include features (including necessary sensors) to ensure that there is no "tailgating" or "crossovers" during the process of passing through the ABC System;	**Compliant** Please ref. to chapter 2.4 and chapter 2.4.2
1.4. Full hardware modularity for configuring single-row or multi-row gates;	**Compliant** Please ref. to chapter 2.3.9
1.5. Access gates (entry and exit) must be swing doors or functionally equivalent, equipped with linear motors.	**Compliant** Please ref. to chapter 2.3.4
1.6. Sensors must be positioned to detect and alert passengers to objects left behind (e.g., luggage, etc.) in the ABC System's control area	**Compliant** Please ref. to chapter 2.3.6
1.7. The ABC System must be designed as an open structure that avoids a feeling of confinement and claustrophobia and provides optimal visibility for the inspector;	**Compliant** Please ref. to chapter 2.2.1
1.8. The exit barrier must be high enough so that a passenger required to undergo standard border control (at the counter) cannot bypass or jump over it;	**Compliant** Please ref. to chapter 2.3.4 and chapter 2.3.5
1.9. The ABC System must be designed to be safe for passengers, such as by avoiding sharp objects/elements, using smooth finishes, and rounded edges, etc.;	**Compliant** Please ref. to chapter 2.2.1, chapter 2.3.4 and chapter 2.3.5
1.10. All materials used in the ABC System must be certified for use in aviation terminals in accordance with safety and health standards;	**Compliant** Please ref.to chapter 2.3.1 And declarations as per "Call for Bids" № 18
1.11. All electronic and mechanical components (such as circuit boards, motorized hinges, etc.) must be concealed where possible and secured;	**Compliant** Please ref. to chapter 2.2.1
1.12. The ABC System must be vandal-proof, scratch-resistant, and protected against foreign materials such as chewing gum, beverages, spilled water, cleaning fluids, etc.	**Compliant** Please ref. to chapter 2.3.1
1.13. In order to protect the biometric data and travel documents processed by the ABC System, the Supplier shall comply with the following minimum cybersecurity requirements:	**Compliant**

a) All communications between the ABC System and the IGPF's IT infrastructure (including web services) will be secured using TLS 1.2 or higher, with digital certificates issued by a recognized certification authority;	Please ref. to chapter 2.4.4
b) Access to the administration interface and monitoring stations will be protected by multi-factor authentication (MFA) and role-based access control (RBAC) policies. Details regarding integration with an existing directory (e.g., LDAP/AD) or the implementation of a proprietary system with integrated MFA will be determined together with the Beneficiary during the design phase, depending on the available infrastructure;	**Compliant** Please ref. to chapter 2.4.5
c) All locally logged and captured data (images, logs, events) must be encrypted at the disk level (AES-256 or equivalent), with the option to configure the retention period;	**Compliant** Please ref. to chapter 2.4.6
d) The supplier shall ensure that all software components adhere to the "secure-by-design" principles and shall be subject to penetration testing and security audits;	**Compliant** Please ref. to 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. to chapter 2.2.1
f) The supplier shall provide proof of compliance with the ISO/IEC 27001 standard for information security.	**Compliant** Please refer to attached ISO 27001 certificate
2. General requirements for operating the ABC System Citizens of the Republic of Moldova who are at least 18 years of age and are not accompanying minors constitute the primary eligible group for crossing the state border via the ABC System. Depending on changes in the regulatory framework, the General Inspectorate of Border Police will determine which citizens are eligible to use the ABC System. In this regard, the ABC System must provide the flexibility and technical capability to expand the categories of persons who can cross the state border using the ABC System.	
2.1. The process of integrating with the ABS (steps, actions/processes, information, communication API, informational messages, etc.) will be jointly developed by the Beneficiary and the Bidder; however, the Bidder must also describe at least two different integration processes (integration processes used in other implemented projects, best practices);	**Compliant** Please ref. to chapter 2.4.3
2.2. Communication between the ABC system and the IGPF data and application server must be via SOAP-based web services;	**Compliant** Please ref. to chapter 2.4.1
2.3. The information systems (applications) within the ABC System must store audit/log data for all actions that take place during the border control process. The audit/log data (in the form of files stored locally on the ABC System's processor disk) must be retained for no more than 7 days;	**Compliant** Please ref. to chapter 2.4.6
2.4. Control/equipment requirements for the entry process into the ABC System: The first barrier (entry gates) at the ABC Depot must support the following operations/features: 2.4.1. A device for reading biometric travel documents, minimum technical requirements in Annex 2;	**Compliant** Please ref. to chapter 2.3.10
2.4.2. A monitor/tablet (small in size) designed to display information that guides the passenger during the process of reading the biometric travel document and to display the results (such as eligibility to use the ABC System, etc.) based on information received from the ABC System;	**Compliant** Please ref. to chapter 2.3.13 and chapter 2.4.2
2.4.3. Entry barrier (2 swing gates) and sensors that ensure only one person enters in the second stage (in the "trap/work" zone for people), when entry is permitted. The minimum technical requirements for sensors are described in the "Safety and Security" section;	**Compliant** Please ref. to chapter 2.3.6
2.5. Control/equipment requirements for the exit process from the ABC System: The second barrier (exit gates) of the ABC System must support the following operations/equipment:	
2.5.1. Hardware-software system for capturing passenger facial images with the following minimum technical requirements (in accordance with ICAO requirements):	**Compliant** Please refer to chapter 2.3.12 and chapter 2.2.1

2.5.1.1. "Active liveness" detection based on 3D imaging technology;	**Compliant** Please ref. to chapter 2.4.7
2.5.1.2. Facial image capture must support (automatic adjustment) for varying passenger heights and be capable of capturing the image when the passenger is standing;	**Compliant** Please ref. to chapter 2.3.12
2.5.1.3. The system must be equipped with a "digital mirror" to assist the passenger during image capture. Additionally, the passenger must receive the necessary instructions on a monitor/screen, including graphical instructions. All information provided must adhere to "user-friendly" practices;	**Compliant** Please ref. to chapter 2.3.12
2.5.1.4. The face detection algorithm must continuously analyze the video feed from the camera to detect the passenger's face. As soon as the passenger's face is detected at the correct distance an algorithm (computational process) for quality assessment must run to verify that the facial image meets the minimum criteria based on ISO 39794-5 and ISO/IEC 19794-5:2011 "Facial image (eye distance, blurring, focus, position, expression)";	**Compliant** Please ref. to chapter 2.4.7
2.5.1.5. The system must be equipped with an anti-identity theft protection system, “Anti-spoofing Control,” which prevents attempts to submit facial images, photographs, or videos;	**Compliant** Please ref. to chapter 2.4.7
2.6. The system must have a switch/button that allows the passenger to request assistance from the inspector.	**Compliant** Please ref. to chapter 2.3.5 and chapter 2.4.1
2.7. The information system designed to manage/operate all IT processes related to border control within the ABC System must offer a wide range of configurations for all stages.	**Compliant** Please ref. to chapters 1 and 2
3. Safety and security	
3.1. The ABC system must be equipped with sensors capable of detecting a range of safety-related conditions and requirements, including:	**Compliant** Please ref. to chapter 2.3.6
3.1.1. The ability to distinguish between an adult or child walking, plus carry-on luggage, plus suitcases and wheeled bags (being pulled or pushed);	**Compliant** Please ref. to chapter 2.3.6
3.1.2. The ability to detect multiple people (presence sensors, adult, child, adult carrying a child) entering the security zone—tailgating;	**Compliant** Please ref. to chapter 2.3.6
3.1.3. Capability for full-featured tailgating detection (without an additional overhead camera), based on artificial intelligence integrated into the vision system.	**Compliant** Please ref. to chapter 2.3.6
3.1.4. Capability to have radar sensors integrated into the lower section for scanning door areas.	**Compliant** Please ref. to chapter 2.3.6
3.1.5. The ability to detect multiple passengers inside the ABC System (presence sensors), including adults carrying children;	**Compliant** Please ref. to chapter 2.3.6
3.1.6. The ability to detect attempts to force open entrance and exit doors;	**Compliant** Please ref. chapter 2.3.6
3.1.7. The ability to detect a passenger moving in the wrong direction;	**Compliant** Please ref. to chapter 2.3.6
3.1.8. The ability to detect luggage or other unexpected items left inside.	**Compliant** Please ref. to chapter 2.1, chapter 2.4.1 and chapter 2.3.6

3.2. The ABC System must 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 to chapter 2.3.14
3.3. The system must include a "visual signaling" system that provides color-coded visual signals to indicate the system's operational status, such as waiting for the next passenger, busy, out of service (maintenance mode), alarm, etc. The color codes must be established in consultation with the Beneficiary. "Visual signaling" may be provided via a monitor/screen (small size) that must be installed at the first barrier;	**Compliant** Please ref. to chapter 2.1 and chapter 2.3.8
3.4. The ABC System must be designed to provide an average processing time of no more than 20 seconds per passenger.	**Compliant** Please ref. to chapter 2.1
Components of IT systems and network infrastructure—monitoring stations, IT and communications infrastructure (hardware) associated with the ABC system—IT&C equipment necessary for operation—as per Annex 3	**Compliant** Please refer to attached “Appendix 1 - Technical Description of the IT&C Infrastructure”
4. Control and monitoring of the ABC System	
4.1. The ABC System must be equipped with a live monitoring station, located in a control room near the ABC Systems. The monitoring station must provide a detailed overview of the operational status of each ABC System and its performance data. The control panel must include a video monitoring component that provides live images from the CCTV cameras installed in/on the ABC Systems;	**Compliant** Please ref. to chapter 2.3.14, chapter 2.4.1 and chapter 2.4.2
4.2. The monitoring station must allow the inspector to monitor and control a group of ABC Systems from a single workstation. A monitoring station must allow the inspector to view and manage up to 5 Systems at the same time;	**Compliant** Please ref. to chapter 2.4.1
4.3. The monitoring stations will be supplied by the Bidder—2 sets (system unit, monitor, keyboard, mouse, connection cables, UPS, licensed software);	**Compliant** Please refer to attached “Appendix 1 - Technical Description of the IT&C Infrastructure”
4.4. Through the Monitoring Station, the inspector must have full control over the ABC System and be able to open both the entry and exit doors (the door will close automatically after a set time has elapsed or once the passenger has passed through), reset/restart, and activate/deactivate the ABC System;	**Compliant** Please ref. to chapter 2.4.1
4.5. To ensure the efficient operation of the ABC System within the airport ecosystem, the Supplier shall detail the following in its technical proposal: **a)** the method of integration with existing systems, including: • DCS (Departure Control System); • AODB (Airport Operational Database); • FIDS (Flight Information Display System); • RMS (Resource Management System).	**Compliant** Please ref. to chapter 2.4.1
b) the proposed logical architecture of the integration, including data exchange (format, frequency, protocols) and fallback mechanisms in the event of external system unavailability;	**Compliant** Please ref. to chapter 2.4.3
c) clarification of responsibilities for connecting and operating the respective interfaces. The bidder shall detail in the technical proposal the integration method, data types, and protocols, and shall include these integrations in the bid price. Details shall be established during the design phase, in collaboration with the Beneficiary.	**Compliant** Please ref. to chapter 2.4.3
4.6. Power on/off function with hidden switch (key).	**Compliant** Please ref. to chapter 2.3.7
4.7. The main features of the monitoring workstation should be: 4.7.1. Display of data retrieved from the biometric travel document, including the facial image from the CIP and from the visual zone (VZ, on the data page);	**Compliant** Please ref. to chapter 2.4.1

4.7.2. Display, when necessary, of images scanned by the travel document reader in all possible light spectra;	**Compliant** Please ref. to chapter 2.4.1 and 2.3.10
4.7.3. Monitoring and control of the automatic facial recognition process, including the ability to view live images of passengers and perform manual recognition if necessary;	**Compliant** Please ref. to chapter 2.4.1
4.7.4. In the event of a failed identity verification: the ability to configure the system's behavior - either the person is required to leave the gate or is detained until released by an officer.	**Compliant** Please ref. to chapter 2.3.6
4.7.5. The ability to release the person via a key switch (separate for each lane) or through border control software.	**Compliant** Please ref. to chapter 2.4.1
4.7.6. Viewing 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. to chapter 2.4.2
4.7.7. Viewing live video images from the facial camera;	**Compliant** Please ref. to chapter 2.4.1
4.7.8. Real-time monitoring of border control processes, including the status of the ABC System;	**Compliant** Please ref. to chapter 2.4.1
4.7.9. Alerts regarding weather conditions and other notifications (e.g., tracking, abandoned items).	**Compliant** Please ref. to chapter 2.3.6 and chapter 2.4.1
5. Training	
5.1. The Bidder shall provide appropriate training for the Beneficiary's technical team regarding maintenance, as well as the detection and resolution of minor errors (software and hardware);	**Compliant** Please ref. to chapter 3.1.12
5.2. The Bidder is required to provide a local maintenance team physically present in the border control area; the team must be capable of providing support and performing preventive maintenance activities. Remote maintenance via VPN or other means is not permitted, and technical support must be provided exclusively by local personnel certified by the manufacturer.	**Compliant** according to the Scope of work for Maintenance and Support chapter 3.2.1
5.3. The Bidder shall provide user manuals and technical documentation during the implementation of the ABC Systems.	**Compliant** Please ref. to chapter 3.1.17
5.4. The Bidder must provide training for the Beneficiary's staff. Two (2) persons will participate in the training, which will take place at the manufacturer's factory. All expenses related to the training (transportation/travel, accommodation, per diem/meals, etc.) will be borne by the Bidder.	**Compliant** Please ref. to chapter 3.1.7
6. Maintenance and support requirements	
6.1. The Bidder must provide a detailed plan for preventive and corrective maintenance of the ABC Systems, including regular maintenance intervals and fault diagnosis procedures;	**Compliant** Please ref. to chapter 3.1.17
6.2. The Bidder shall supply spare parts for all essential components of the ABC System throughout the warranty period and for post-warranty maintenance;	**Compliant** Please refer to chapter 3.2.5. and declarations as per "Call for Bids" № 17 a), b), c)

6.3. If a major malfunction is identified that affects the normal operation of the ABC System, the Bidder must take action to remedy the malfunction within a timeframe specified in the support agreement, typically no more than 72 hours;	**Compliant** according to the Scope of work for Maintenance and Support chapter 3.2.1
6.4. The Bidder shall provide ongoing training for the Beneficiary's technicians throughout the duration of the ABC System's use to ensure its efficient operation and safety.	**Compliant** according to the Scope of work for Maintenance and Support chapter 3.2.1
7. Commissioning and periodic validation tests	
7.1. Testing the system's full functionality (document capture, facial recognition validation, barrier access control, etc.);	**Compliant** Please ref. to chapter 3.1.13
7.2. Performance testing to verify processing time and passenger throughput per minute;	**Compliant** Please ref. to chapter 3.1.13
7.3. All tests will be documented in a test report to be submitted to the Beneficiary for validation.	**Compliant** Please ref. to chapter 3.1.13
7.4. To validate the interoperability, performance, and compatibility of the ABC System with the existing infrastructure: a) The supplier will implement a functional pilot system for at least 5 ABC gates, including integration with the IGPF infrastructure and testing of biometric capabilities;	**Compliant** Please ref. to chapter 3.1.11.3 and chapter 3.1.13
b) The testing period shall be no less than 30 days, with documentation of all results and any non-conformities;	**Compliant** Please ref. to chapter 3.1.13.1
c) Full commissioning of the other units will be contingent upon the Beneficiary's formal acceptance of the PoC results.	**Compliant** Please ref. to chapter 3.1.15
8. Compliance Requirements	
8.1. All components of the ABC System must comply with ICAO (International Civil Aviation Organization) and IATA (International Air Transport Association) regulations;	**Compliant** Please ref. chapters 1 and 2
8.2. The system must be certified for use in airport terminals, complying with safety regulations and fire safety standards.	**Compliant** Please ref.to chapter 2.3.1 And declarations as per "Call for Bids" № 18
8.3. The supplier shall provide complete documentation regarding the API structure used by the ABC System (methods, parameters, responses, error codes, authentication);	**Compliant** Please ref. to chapter 2.4.3
8.4. The functional and security testing methods applicable to the API will be specified;	**Compliant** Please ref. to chapter 2.4.3
8.5. The supplier shall present a rollback plan in the event of a critical failure following an upgrade of the ABC software (including backups, recovery procedures, and estimated duration).	**Compliant** Please ref. to chapter 3.2.4
9. Delivery and implementation Deadlines	
9.1. The supplier shall provide a detailed schedule for the delivery, installation, and commissioning of the ABC Systems, which shall include key milestones and deadlines for their completion;	**Compliant** Please ref. to chapter 3.1.2

9.2. The deadline for the installation and full commissioning of the ABC Systems is 120 calendar days from the date of contract signing;	**Compliant** Please ref. to chapter 3.1.2
10. Reporting and Documentation requirements	
10.1. The supplier must provide detailed reports on the project's progress, updates on testing and validation, as well as any delays or issues that may arise during implementation;	**Compliant** Please ref to chapter 3.1.2
10.2. All documents and reports must be provided in English and Romanian;	**Compliant** Please ref to chapter 3.1.2
10.3. Upon completion of the implementation, the supplier will deliver the complete documentation regarding the system architecture, operational procedures, user manuals, and maintenance guides.	**Compliant** Please ref to chapter 3.1.17
11. Obligations of the Final Beneficiary (General Inspectorate of Border Police)	
11.1. The IGPF will publish a set of APIs (SOAP-based web services) to be consumed/accessed by the ABC System for authorizing passengers to pass through automated border control.	**Compliant** Please ref. chapter 2.4.3
12. Log Retention policy	
12.1. The ABC system will retain log data (system logs, access logs, screenshots) for a minimum period of 30 days, with the possibility of extension or automatic archiving. For budgetary evaluation, the bidder may propose a maximum term, recommended to be 90 days, which will be validated with the beneficiary during the contracting phase.	**Compliant** Please ref. chapter 2.4.6
12.2. Secure deletion policies shall be configurable in accordance with the Beneficiary's internal policies and the provisions of the GDPR.	**Compliant** Please ref. chapter 2.4.6
Annex 2	
Minimum technical requirements for the biometric travel document reader	
A device for automatically reading the entire data page of a biometric travel document, without detachable parts, designed to read data from: the machine-readable zone (MRZ); the visual zone (VZ); the wireless electronic identification circuit (RFID); the barcode, comparison of the read data, and verification of the travel document's authenticity through the ability to scan the data page under different light spectra. (White, IR, UF, coaxial, OVD, others).	**Compliant** Please ref. to chapter 2.3.10
Optical document reader	
Scan area, mm ---- 90 x 130 - full passport page; Video sensor type ---- CMOS; Color representation --- RGB; Color depth --- 24 bits; Frame size, pixels --- 4200 x 3120; Number of megapixels ---13;	**Compliant** Please ref. to chapter 2.3.10
Contactless electronic identification circuit reader:	
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. to chapter 2.3.10
Reading and image processing of documents format:	
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);	**Compliant** Please ref. to chapter 2.3.10

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.	
Machine Readable Zone (MRZ) Supported formats of the Machine-Readable Zone (MRZ) in accordance with the ICAO 9303 standard. Searching for the Machine-Readable Zone on the document image; Recognition in the white light and infrared spectrum; Verification of the check digits to ensure that the machine-readable zone has been filled out correctly in accordance with ICAO 9303 requirements. Assessment of the accuracy and quality of printing, in accordance with ICAO 9303 1-1, ISO 7501, 1831, 1073-2.	**Compliant** Please ref. to chapter 2.3.10
Barcode reading: Maintained formats: 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	**Compliant** Please ref. to chapter 2.3.10
Automatic document type determination 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.	**Compliant** Please ref. to chapter 2.3.10
RFID SDK/Functionality 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	**Compliant** Please ref. to chapter 2.3.10
Required mandatory security functionality: - 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.	**Compliant** Please ref. to chapter 2.3.6 and 2.3.7
Analysis and comparison of textual information Areas of the document whose data will be analyzed (compared): - machine-readable area - visual area	**Compliant** Please ref. to chapter 2.3.10

- RFID electronic circuit	
Authenticity verification - Luminescence check (UV Dull Paper): banquette, MRZ, photo location area; - MRZ print contrast check in accordance with ICAO standard 9303 (IR B900 Ink) Checks available after document type determination: - Check for patterns of certain colors and shapes in the white, infrared and ultraviolet light spectrum (Image Pattern); - check the illumination of fibers of a certain color and size (UV Protection Fibers) - checking for False Luminescence (False Luminescence) - Checking the method of photo embedding: printing or pasting (Photo Embedding Type) Checking the visibility in the infrared spectrum (IR Visibility): - white elements - textual data - photo (basic and additional) - checking for holograms (OVD) - reading luminescent text and comparing with data read from the machine readable zone MRZ or visual area VIZ (OCR Security Text) - Invisible Personal Information (IPI) visualization - checking retro reflective protection - bar code format verification.	**Compliant** Please ref. to chapter 2.3.10
Annex 3	
Components of IT systems and network infrastructure – monitoring stations, IT and communications infrastructure (hardware) associated with the ABC system – IT&C equipment necessary for operation.	**Compliant** Please refer to attached “Appendix 1 - Technical Description of the IT&C Infrastructure”

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 e-Gates & Kiosks.

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

Compliancy 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 (NESC), 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 e-Gate, 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, Nikola 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 allow 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 provides 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 allows 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.

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.

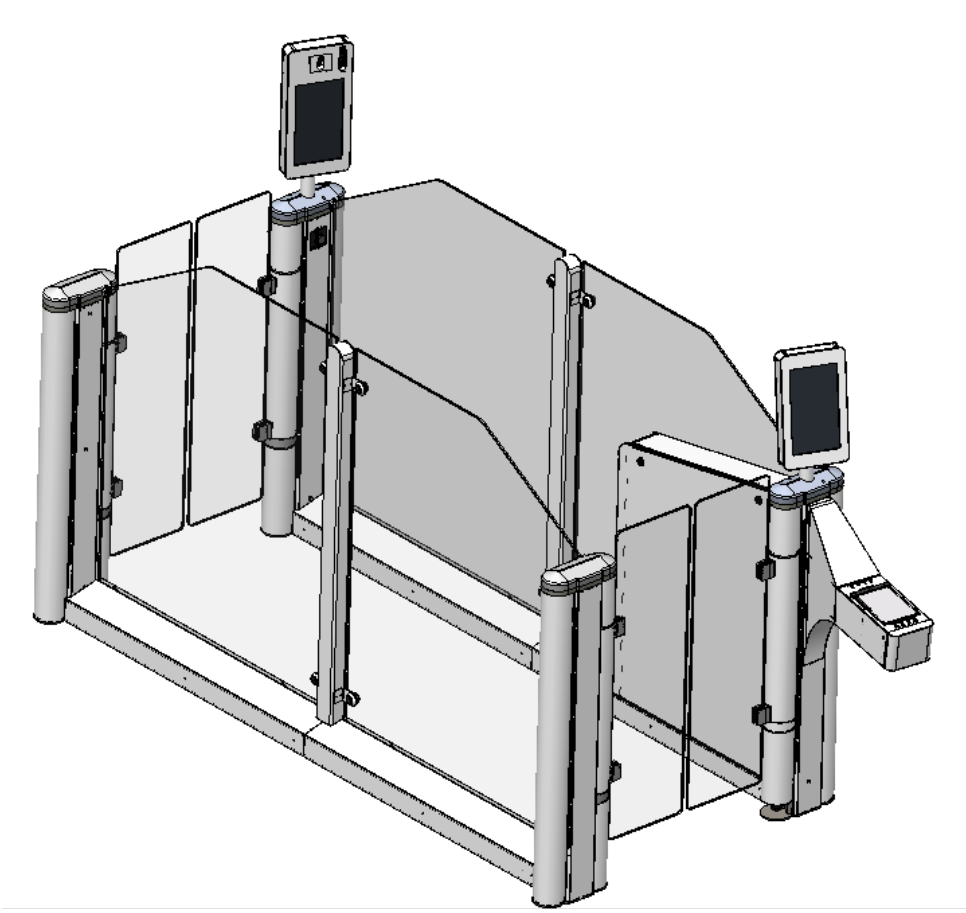
2.2 Technical Description of the e-Gate Solution

2.2.1 Basic Double Door FastGate

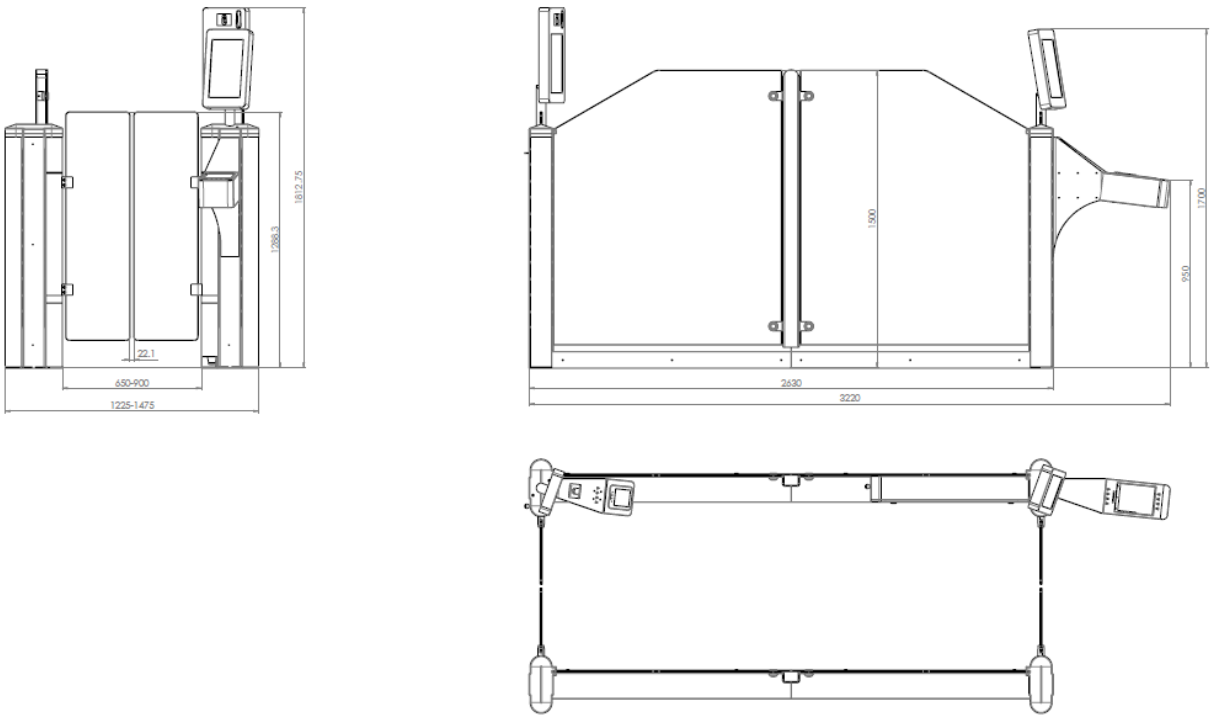
The MB Double Door FastGate series, designed according to the Frontex best practice technical guidelines for ABC systems, combines modern, cost-efficient design and latest technology to accelerate and secure border control. Based on a user-centric approach the Double Door FastGate supports all eMRTD, 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.

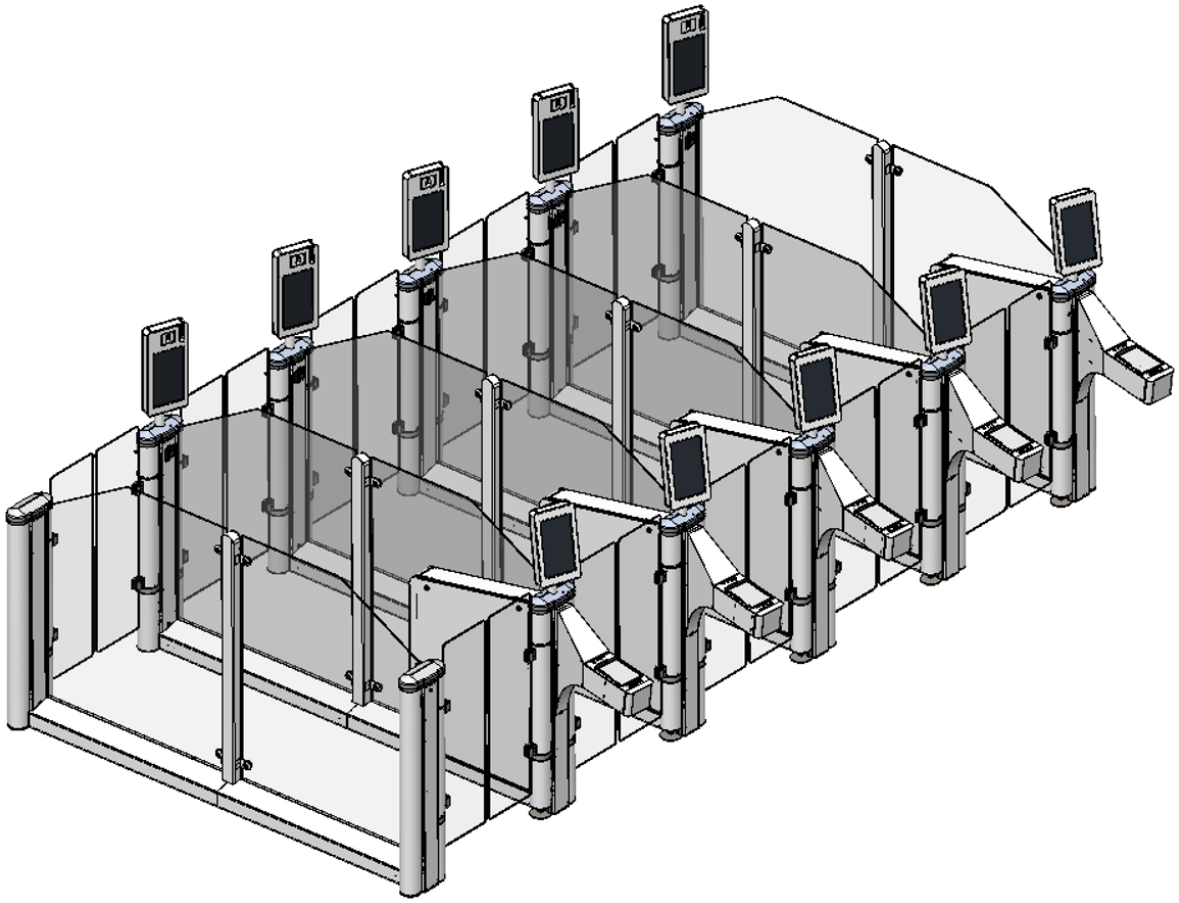
The objective of the Double Door FastGate solution is a significantly increased security and a reduction of the workload of the controller, like police or security personal. In addition, in its latest generation offers the Double Door FastGate series the most flexibility, high modularity, cost-efficient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



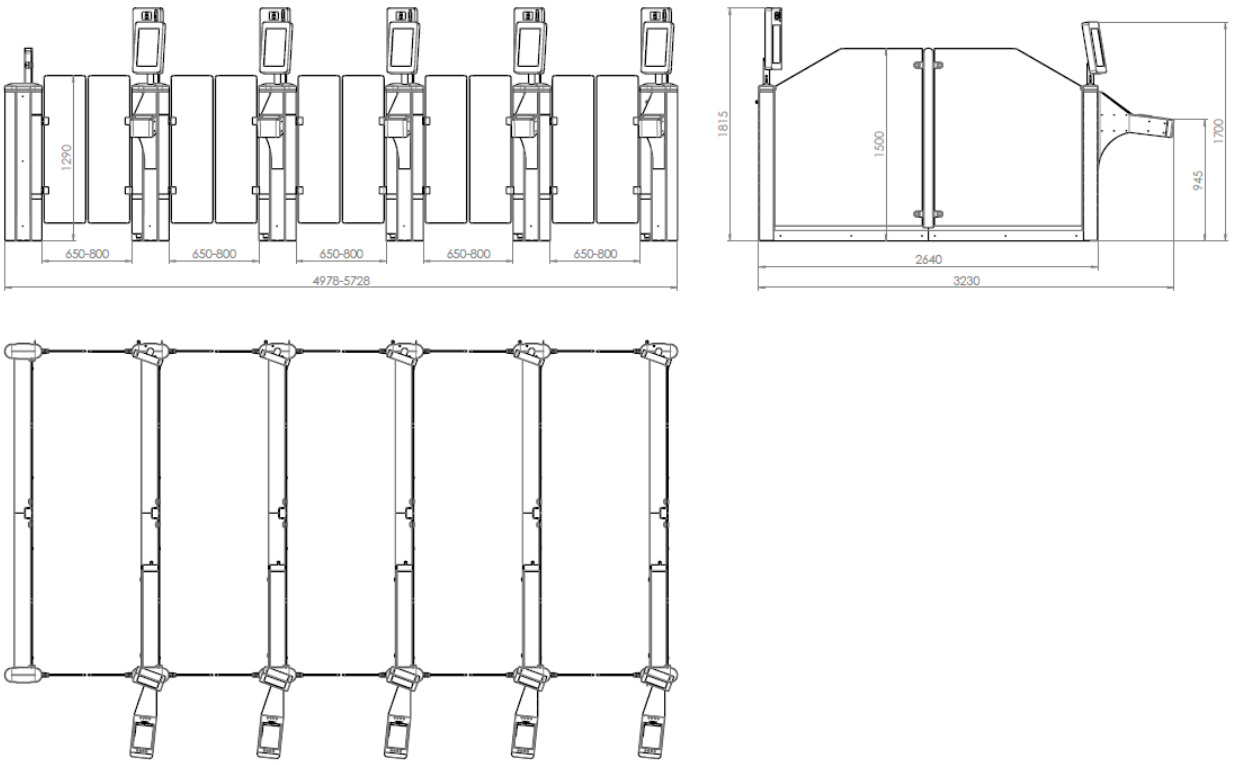
Proposed design of a Single Lane Double Door Fast Gate



Proposed dimensions of a Single Lane Double Door Fast Gate



Proposed example of a Five Lane Double Door Fast Gate



Proposed dimensions of a Five Lane Double Door Fast Gate

The Double Door FastGate represents 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:

- Passport reader
- Smart card reader
- Barcode reader
- Face verification
- Iris scan
- Fingerprint reader

2.2.2 Scope of Work for Components Provision

This chapter illustrates high-level break down of Scope of Work for Components Provision between RSD & Mühlbauer.

Component Provision	Responsible		Description
	MB	RSD	
MB Fast Gate – Hardware	X		2.3 MB Fast Gate - Hardware
MB Fast Gate – Software / Control and monitoring of the ABC System	X		2.4 MB Fast Gate – Software / Control and Monitoring of the ABC System
IT SW & IT HW for Main Data Center		X	Components of IT systems and network infrastructure – monitoring stations, IT and communications infrastructure (hardware) associated with the ABC system – IT&C equipment necessary for operation according Annex 3.

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

APC Back UPS Pro BR16000SI

- Output power: 960W – 1600VA, 230VAC, sine wave, 8 x C13
- Dimensions: 260mm x 100 mm x 368 mm,
- Weight: 12.1 kg
- Topology: Line Interactive
- Battery: Included, Sealed, Lead-Acid, maintenance free
- Compliances: A-Tick, C-Tick, CE, EAC, RCM, TIS I
- Certifications: EN/IEC 62040-1:2019/A11:2021 standard EN/IEC 62040-2:2006/AC:2006 standard EN/IEC 62040-2:2018 standard

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 to move 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, System behavior, alarms & security

- AI based 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 integrated into lower section for scanning door areas; the sensors can track the position of the traveler and luggage 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.
- in the event of a failed identity verification, the system behavior is configurable to either instruct the person to leave the gate area or place the individual under detention until release by an authorized officer, in accordance with operational procedures defined by the client.
- 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.
- MB e-Gate is equipped with an emergency button located within the mantrap zone, enabling passengers to request assistance from authorized personnel with a single press when needed.

2.3.7 Key Switch

MB e-Gate is equipped with two key switches on exit side. The ON/OFF switch and its functions are hidden on the exist side.

1. **First Key (Normal Operation Key)** with three positions (momentary) provide following functions:
   - Middle Position (0) is position from which key can be taken out only.
   - Position 1 (short turn) – Send signal to Start Up the e-Gate, when released key goes back to Position 0. After some time, if the e-Gate was OFF the e-Gate will be Turned ON, if the e-Gate were ON it will not change the state.
   - Position 1 (5 second hold) – Send the signal to PLC and Machine Software for starting Shut Down Procedure of the Gate, when released key goes back to Position 0. After some time e-Gate will Shut Down.
   - Position 2 – Send the signal to PLC and Machine Software to open Entrance Doors to release passenger, when released key goes back to Position 0, after the passenger leaves the e-Gate, Entrance Doors automatically closes and e-Gate is ready for new passport evaluation.
2. **Second Key (Service Key)** with three positions (maintaining) provide following functions:
   - Middle Position (0) is position from which key can be taken out only, and doesn't change any state of the e-Gate
   - Position 1 – Set the Entrance Door motors and brakes powerless. Doors will free to be manually open or closed, when released key hold the Position 1.
   - Position 2 – Set the Entrance Door and Exit Doors motors and brakes powerless. Both Entrance and Exit Doors will free to be manually open or closed, when released key hold the Position 2.

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), and other preferable colors defined by Customer
- LED´s at Bio Devices for User Guidance and convenience

2.3.9 Modularity

- All components are easily removable and can replace in very short time are covered and not accessible from outside.
- Parts like monitors, document reader, 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).

The document reader is to be integrated into automatic border security kiosks and other data acquisition systems. The device is constructed in plastic body with a glass top (it can be made of high-resistant glass). The level of protection provided by the device body in the area available to the user (glass) corresponds to IP54 class. 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. The device is supplied with software development kit (SDK) for easy integration into existing end-user systems.

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 • 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
Machine readable zone (MRZ)	

Supported MRZ formats	• 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

Features	• 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
Barcodes	
Supported formats	• 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
Authentication	• Barcode format check
Automatic document type recognition	
Order of document type recognition	• Country→Type→Series

Features	• 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

Graphic fields processing	
Types of graphic fields	• Portrait of the document holder • Signature • Barcode • Fingerprint, etc.
Features	• Cropping and displaying graphic fields as separate images in compliance with the sample of the corresponding document • 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
OCR of the visual zone	
Recognition of character sets	• Central European and Eastern European Latin (1250) • Cyrillic (1251) • Western European Latin (1252) • Greek (1253) • Turkish (1254) • Baltic (1257) • Other fonts of any size
Features	• 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
RFID SDK	
Supported RFID-chip Standards	• ISO/IEC 14443-2 (type A and B) • ISO/IEC 14443-3 (MIFARE® Classic Protocol) • ISO/IEC 14443-4
Data access modes	• Direct • BAC

Authentication	• EAC • PACE • SAC • Active (AA) • Passive (PA) • Chip (CA v1, CA v2) • Terminal (TA v1, TA v2)
Supported applications	• ePassport (DG1–DG16) • eID (DG1–DG21) • eSign • eDL (DG1–DG14)
Certificate management	• Local storage • Receiving certificates online through the program interface • Master List, CRL support
Features	• 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
Analysis and comparison of text data	
Document areas for cross-checking of the readout data	• MRZ • VIZ • RFID-chip • Barcode
Verification	• Validity of any dates • Authenticity of names and surnames according to lists of wordstops • Zero numbers of sample documents
Adjustment of formats and measuring units to those used in the user OS	• Date • Weight • Height, etc.
Features	• 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
Authenticity verification	

Operation available for any document	• Checking luminescence (UV Dull Paper) of:
	  ○ Form
	  ○ MRZ area
	  ○ Portrait area
	• Checking the MRZ print contrast in compliance with ICAO 9303(IR B900 Ink)

Operations available after document type recognition	• 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
Additional SDK functions	
Image formats	• *.BMP • *.JPG • *.JP2 • *.PNG • *.TIF • other image formats are possible on request

Interoperability	• 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»

OS compatibility	• Windows 7 (x86, x64), Windows 8, Windows 10, Windows 11, Ubuntu 20.04—24.04, Debian 11—12, RHEL 9, macOS 11+
Drivers	• Microsoft certified
Features	• Simultaneous optical scanning and RFID chip reading • Firmware upgrade via USB interface (automatic upgrade after installing new SDK version) • Multilingual interface
Software updates	
SDK	• Twice a year
Document template database	• Monthly
Functionality	
Optical Reader Light Sources	• White • Infrared 870 nm • Ultraviolet 365 nm • Coaxial White
Reader of radio frequency identification devices (RFID)	• Included
Number of megapixels	• 13 MPx
Resolution, ppi	• 710+/- 3%
Frame size, pixels	• 4200x3120

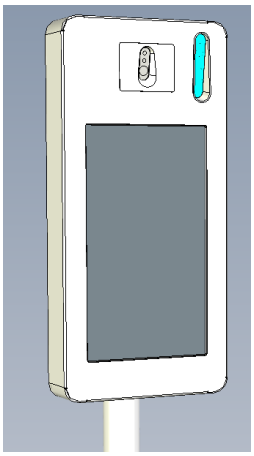
Note: In case not all the features are listed, please note that the document reader will meet the criteria of Annex 2.

2.3.11 Option: Smartcard Reader

The OMNIKEY® 3121 is a high-performance, USB contact smart card reader, compliant with all industry standards.

- **Standards** – ISO 7816 & EMV2 2000 Level 1
- **Host Interface** – USB 2.0
- **Operating System Support** – Windows Vista/7/8/8.1/10, Windows CE 6.0, Android, Mac OS X, Linux
- **Card Size** – ID-1 (Full Size)

2.3.12 Biometric face camera



- Mühlbauer uses a wide-angle camera for face recognition with 4K resolution, High Dynamic Range (HDR) and auto adjust feature according to ICAO requirements.
- 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 is used for user guidance and instructs the face verification process to travelers e.g. verification successful or failed etc.
- Digital Mirror and on-screen Face Verification silhouette functionalities are included in Face Verification unit
- 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 and Liveness detection are included

2.3.13 Monitor/Display

- 13.3" front and 15"on the back
- Full HD
- Touch technology – capacity
- Edge to edge glass
- Anti-fingerprint coating
- Representation of the travel documents on document scanner

The small monitor in front 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 is 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.
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 entry 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, on the monitor graphics will be shown to direct the traveler to manual inspection.
If the passenger leaves his passport on the document reader, then the e-Gate 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 user is shown on the monitor to move to manual passport control.
On the second bigger monitor live face mirroring is shown while passenger is in internal space of the e-Gate. If the Face Verification process is successful pictures doors are opening and passenger is free to go. In the case that Face Verification Process is not successful, Border police officer could intervene through MB BGCU software or animation for manual control will be shown.

2.3.14 CCTV

- FastGate installed area can be observed through additional CCTV camera.
- A dome camera is installed on top of each e-Gate in order to allow full surveillance of the persons passing and activities inside the e-Gate.
- 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 e-Gate 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/m²

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 is included in the e-Gate.

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

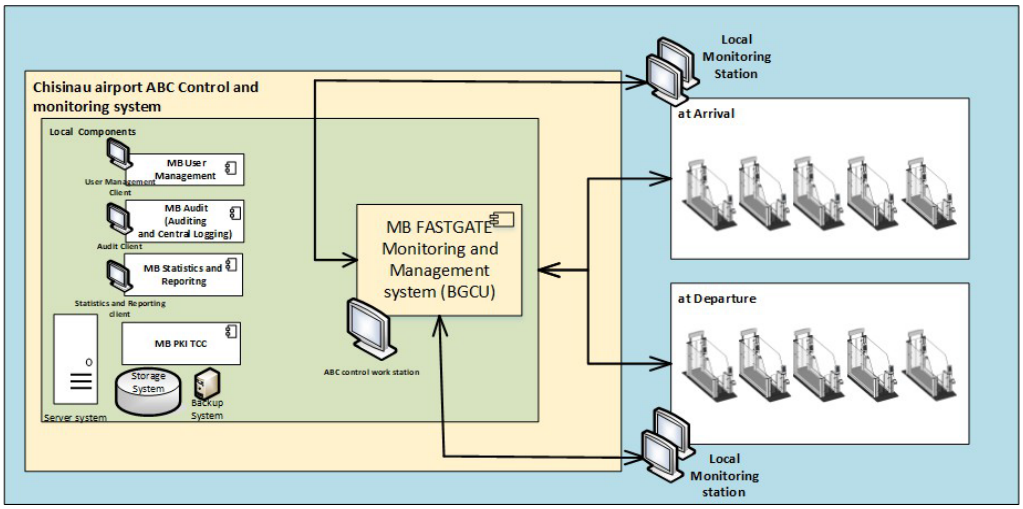
This proposal has been developed to supply, Installation and Commissioning of ABC Gates at Chisinau International Airport. The e-Gate is design based on state-of-the-art technology fully capable of scanning and verifying electronic document (e.g. ePassport, eID etc.) against respective template, reading chip information, performing various biometric verification including facial as well as tailgating detection and prevention. In order to complement the e-Gate 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 e-Gate. Its instance is running on the server located within server room and accessible via browser. It allows border police to perform various operations including initiation, activation and monitoring current process happening at the e-Gate 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 specifications, 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 administrators to manage and monitor personnel and assign access to related systems accordingly.

All e-Gate, servers and workstations will be set up at location specified by client and connected to local network using Ethernet connection.
The offered software components ensure system resilience against potential threats by adhering to recognized best practices for secure architecture, thereby enhancing operational reliability and ensuring compliance with applicable industry standards. Furthermore, it also ensures that all offered software components are developed and maintained in accordance with "secure-by-design" principles and subject to regular penetration testing and comprehensive security audits to maintain the overall security posture of the system.
The ABC solution undergoes periodic security testing, including penetration testing, performed by the manufacturer as part of its secure development lifecycle. Any identified vulnerabilities are remediated and addressed through patches and updates provided to ensure continuous security of the system.

The delivery of this project includes

- Automated Border Control e-Gate in technical specification document. Mandatory components include
  - Double door
  - Document reader
  - Facial verification camera
  - 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 implementation (exemplary)

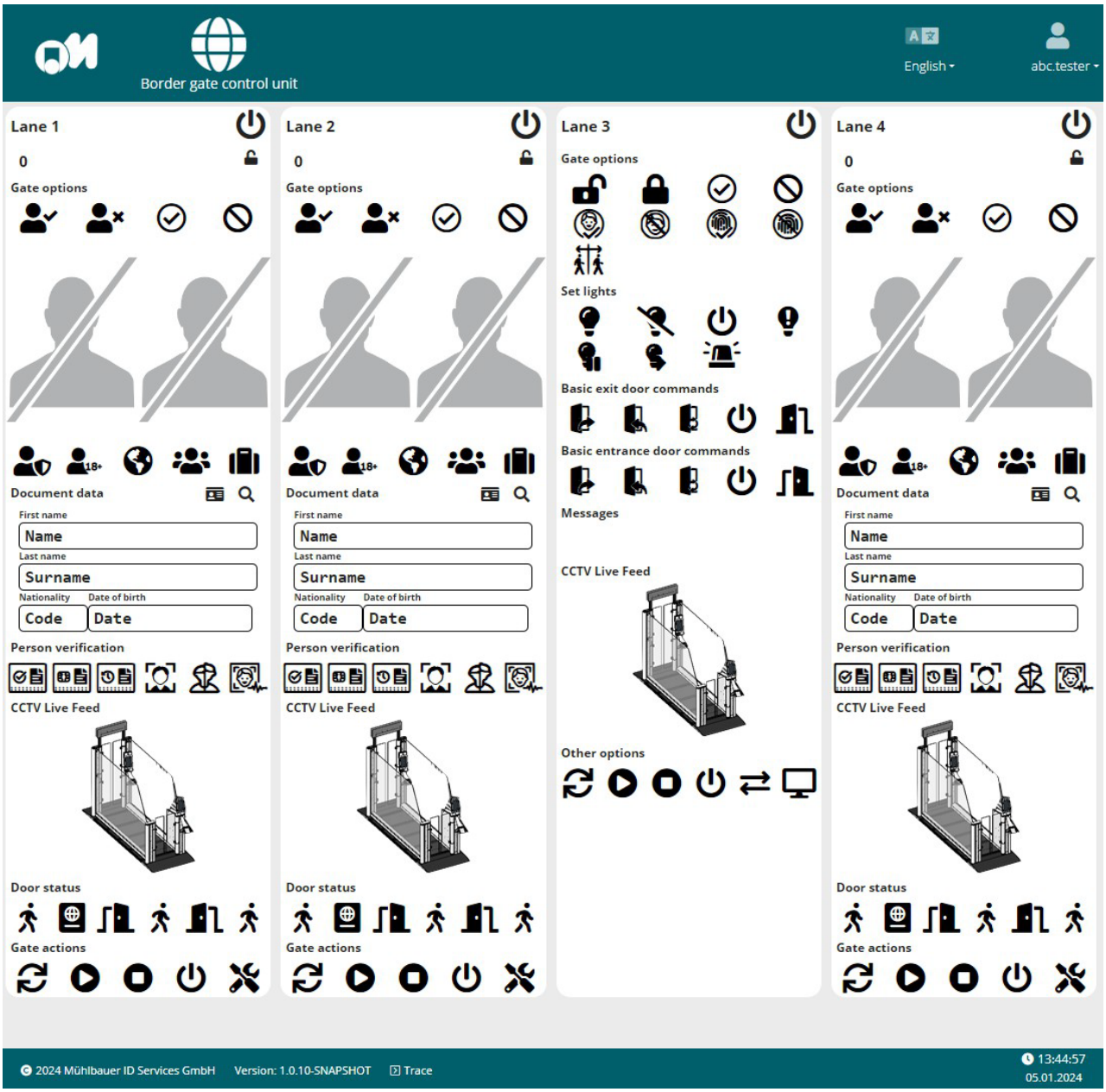
2.4.1 Border Guard Control Unit (MB BGCU)

The MB e-Gates are delivered with the management module for the border police to monitor and control the e-Gate 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 e-Gate 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 e-Gate. A separate section on the monitor is provided for every connected MB e-Gate. 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 has full control of the ABC System and 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 e-Gates.



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 e-Gate 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:

- The BGCU displays data retrieved from the biometric travel document, including document data read from the chip (CIP), the facial image stored in the chip, and the facial image from the visual zone (VZ) on the document data page for operator review and processing. The system presents the overall result of the border control process using clear color indicators, where document validation fields turn green or red depending on the validation outcome, and biometric verification and watch-list check results similarly change status when the passenger enters the gate. Retrieved information, including biometric data and verification results, is displayed during processing and transmitted via web interface to the client-designated system for further use. No biometric information or verification results are stored locally within the BGCU.
- 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 border 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 e-Gate 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 workstations including the status of the ABC system. 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.

Method of Integration with the existing systems:
The BGCU system is built to connect smoothly with the airport's existing environment, including systems like DCS, AODB, FIDS, and RMS. These systems typically handle core airport operations such as flight data, passenger processing, resource allocation, and information displays.

For integration, the approach relies on the technical interface specifications provided by the existing systems. These specifications define how data should be structured and exchanged so that both sides can communicate correctly.

The BGCU system provides standard web service interfaces using REST and SOAP protocols. These are used in two main ways:

- To receive operational data from airport systems.
- To send back responses such as confirmations, processing results, or error/exception messages to the relevant system.

Depending on the situation, data can be exchanged in real time or in a request-response manner. Information is typically formatted in common standards like JSON or XML so it can be easily understood by different systems.

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 e-Gates have an emergency switch/button that allows the passenger to request assistance from the inspector. The emergency switch is triggering an alarm but it does not automatically release the barriers. The inspector is 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;

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 are also provided in the form of interface specifications

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 e-Gate system against the National Border Control System or other external systems.

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 shall 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.

The proposed BMA interface architecture is based on a service-oriented integration layer enabling secure and standardized data exchange between the BGCU system and external airport systems. Data interchange is implemented using REST and SOAP web services, with payloads structured in JSON or XML formats depending on the interfacing system capabilities. Data transmission occurs in both real-time (event-driven) and near real-time request/response modes, with configurable polling intervals where applicable.

If an external system becomes unavailable, the solution uses a message queue to temporarily store data so no information is lost and processing can be completed later. It also includes automatic retry attempts, timeout controls, and backup routing paths to keep operations running smoothly. Once the connection is restored, all stored data is processed to ensure everything is fully synchronized.
MB confirms that integration with external systems is included within the proposed solution, and the associated API development and integration effort is included in the bid price. Responsibility for providing the interface specifications, including data structures, communication protocols, message formats, and connectivity requirements, remains with the respective system owner for each interfacing system.

Based on the approved interface specifications, MB shall design, develop, configure, and implement the required APIs and interface connections to enable secure, reliable, and scalable data exchange with the respective systems.

MB shall be responsible for the full lifecycle of BGCU-side integration components, including development, testing, deployment, and ongoing support, while coordination related to access provisioning, endpoint availability, and overall readiness of third-party systems shall remain the responsibility of the respective external system owners.

The integration process with the ABS, including all relevant steps, actions, data flows, communication APIs, and informational messages, shall be jointly defined and agreed upon between the Beneficiary and the Bidder.
A description of at least two alternative integration approaches, based on prior project experience and established industry best practices, will be provided during the project implementation and implementation specification phases, including their application within the system architecture to ensure flexibility, robustness, and alignment with proven and reliable methodologies.

For example:

- a real-time, API-based synchronous integration approach enabling immediate data exchange and validation between systems
- an asynchronous, message queue–based integration approach ensuring resilience, scalability, and reliable data processing in distributed environments.

Final interface details, integration methods, data types, protocols, and operational responsibilities will be confirmed and refined during the design phase in close collaboration of both parties.

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.

All communication between the IGPF's infrastructure and the ABC gate is secured using TLS 1.3, with digital certificates, ensuring protection of biometric data and travel documents processed by the ABC System in compliance with cybersecurity requirements.

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

The offered User Management is offered with two-factor authentication for limited users. 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 e-Gate 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 record 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.

In addition, all data captured and processed by the ABC System—including images, logs, events, and audit records—is protected through a comprehensive, multi-layer encryption architecture provided as part of the delivered solution. Data at rest is encrypted using industry-standard algorithms such as AES-256 (or equivalent), implemented at the storage layer within the IT&C infrastructure (IBM FlashSystem 5300 see Annex 3 "Technical Description ITC"), with optional support for host-level encryption mechanisms (e.g., BitLocker), depending on the deployment scenario. Data in transit between system components is secured using strong cryptographic protocols (e.g., TLS 1.2/1.3), ensuring protection against interception and unauthorized access. Cryptographic key management is implemented through secure and standardized mechanisms, including hardware-based protection via Trusted Platform Module (TPM), with the capability to integrate external key management systems, such as Hardware Security Modules (HSM), if required by the Beneficiary.

2.4.7 Liveness Detection System

In order to be protected against spoofing attack, our **facial and fingerprint** 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.

The proposed face detection continuously analyzes the live video stream from the camera using an advanced face detection algorithm to reliably detect the passenger's face in real time. Once the face is positioned at the correct distance, an automated quality assessment process shall be triggered to ensure that the captured facial image complies with the minimum requirements defined in ISO 39794-5 and ISO/IEC 19794-5:2011, including parameters such as eye distance, sharpness, focus, positioning, and facial expression.

A conventional face identification system can be deceived by presenting a photograph to the camera, just as fingerprint systems can be compromised using fake fingerprints. The proposed BGCU system, combined with the PAD system, helps prevent such security breaches by determining whether a face captured in a video stream or a single frame is a live subject or a photograph. Liveness detection can be performed in passive mode, while active liveness detection based on 3D imaging technology provides an additional layer of security by verifying depth and facial structure to detect spoofing attempts.
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	**MB e-Gates:** • Document Reader • Face Camera with Face Liveness Detection • CCTV • Facial Verification	10	
2	**Software License:** • 1x Border Guard Control Unit software license • 1x Border Management Adapter software License (API) • 2x Terminal Control Center software license • 1x User Management Software License • 1x Audit software • NEUROtechnology liveness detection image technology	1	

3 Services for ABC e-Gates

3.1 Implementation Services

3.1.1 Scope of Work for Implementation Services

This chapter illustrates high-level break down of Scope of Work for Implementation Services between RSD & Mühlbauer.

Provision	Responsible		Description
	MB	RSD	
Project Initiation & Project Management		X	Clarification of technical requirements
		X	Project coordination (operational meetings)
		X	Support in clarification of technical requirements
Necessary building refurbishments		X	Any kind of necessary works related to Installation Facilities, Communications and Civil Works in Moldova
Procurement of Necessary IT SW & IT HW for Main Data Center		X	Procurement & Delivery of Specified IT HW & SW for Main Data Center to its final installation place at customer in Chisinau in Moldova
Installation of procured IT SW & IT HW for Main Data Center		X	Installation of IT HW & SW for Main Data Center to its final installation place at customer in Chisinau in Moldova; connection to the customer environment as required by the tender.
Audit of installed IT SW & IT HW for Main Center	X		MB team will audit of installed Main Data center by MB employee for 3 days in presence of RSD in Chisinau, Moldova
		X	RSD is responsible to correct all findings in shortest time possible and in full compliancy with tender requirements and with given deadlines and instructions from MB side.
Training at Mühlbauer Facility in Germany for RSD	X		Trainer for Training by MB for RSD Engineers at Mühlbauer Facility in Roding, Germany: - 3 days for software solution - 4 days training for e-Gate Hardware - 1 days for IT
		X	Trainees: 2 (two) machine service engineers from RSD side, experienced in mechatronics, electronics, mechanics, IT networks and basic programming skills; For the duration of the training. It is recommended to stay for the FAT and customer training. RSD has to cover all travel, accommodation and local costs during stay in Roding, Germany
Pre-commissioning at MB facility in Roding	X		Pre-commissioning and preparation for Factory Acceptance Test (FAT) in Roding for 10x e-Gate HW & Software (please note that software will be installed on Test servers from Mühlbauer)

Training provided to Staff of Customer	X		Training for customer: e-Gate Operation and Basic Maintenance (2 days in Roding) Including travel and accommodation costs for customer trainees (2 persons)
FAT	X		FAT with customer: 2 persons (2 days in Roding) Including travel and accommodation costs for customer FAT delegation (2 persons)
Delivery from Mühlbauer in Roding/Germany to Moldova at place of installation	X		Logistics and transportation on terms of CIP Chisinau International Airport, Moldova
Domestic logistic		X	• Customs clearance, transport to respective site, potential needed temporary storage of goods, adequate storage of goods to avoid damages; • Carry out all logistics in Moldova after customs clearance (distribution to installation location);
		X	• Temporary storage at a local warehouse in Moldova;
SAT and Commissioning phase in Moldova	X		• On-site equipment installation and integration for 5 psc. **in piloting process**, including: - Physical setup of the e-Gate systems and ITC infrastructure; - Electrical and network interconnection; - Configuration checks of hardware and software systems; - System startup and functional verification prior to SAT.
		X	• Assistance in on-side equipment installation and integration **in piloting process,** including: - Physical setup of the e-Gate systems and ITC infrastructure; - Electrical and network interconnection; - Configuration checks of hardware and software systems; - System startup and functional verification prior to SAT.
		X	• On-site equipment installation and integration **for rest of 5 psc.**; - Physical setup of the e-Gate systems and ITC infrastructure; - Electrical and network interconnection; - Configuration checks of hardware and software systems; - System startup and functional verification prior to SAT.
	X		• Support in On-site equipment installation and integration **for rest of 5 psc**; - Physical setup of the e-Gate systems and ITC infrastructure; - Electrical and network interconnection; - Configuration checks of hardware and software systems; - System startup and functional verification prior to SAT.
Ramp-Up Support		X	• Ramp-up technical support (5 days on-site/Monday - Friday, 8h / day). Provision of sufficient technical staff to provide the ramp-up support. If required by the customer.

Training for Customer at Customer Facility		X	• In order to train technical team of customer nominated to perform basic maintenance activities of the equipment & software at Chisinau International 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)

3.1.2 Preliminary Project Plan

This chapter illustrates initial project plan.
Project plan (**Attached Appendix 2 - Preliminary Project Plan**) highlights major milestones containing various steps resulting in project implementation. This is initial version of project plan, detailed project plan will be provided after contract signature.

Project reporting and documentation

Reporting methodology will be agreed during project kick-off with customer team. Detailed reports on the project's progress, updates on testing and validation, as well as any delays or issues that may arise during implementation will be provided. All project related documentation will be provided in English and Romanian language.

3.1.3 Project Initiation

A Kick-Off meeting between the Mühlbauer 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.
Mühlbauer team is meeting remotely with Customer to clarify (among others) the following topics:

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

Mühlbauer will support RSD remotely in regards to the project initiation with following resources:

- 1x Project Manger
- 1x Solution Architect
- 1x Service Manager
- 1 day, 8 hours per day
- Available remotely during business hours, Mon.-Fri. 08:00-17:00 CET

3.1.4 Installation Facilities, Communications and Civil Works

When applicable, RSD with Customer shall be responsible for any design, physical construction works, civil works, fit-out or connections (electricity, communications, etc.) and other related activities required for the installation & operation of the systems. It is out of scope of Mühlbauer.

3.1.5 Pre-Commissioning at Mühlbauer Facility

For the preparation for the Factory Acceptance Test of the proposed equipment and software solution, Mühlbauer will pre-install the solution. The pre-installed systems will be configured to demonstrate the functionality of the solution at Mühlbauer facility in Roding.
Please note that central / client system software components will be installed on test equipment.

3.1.6 Update Training for RSD engineers in Mühlbauer Facility

During pre-commissioning phase at Mühlbauer facility upon request by Mühlbauer, RSD has to provide engineers with expertise in software engineering, mechatronics and electronics and is IT literate; Mühlbauer will train engineers for:

- Software Components – 3 days
- e-Gate Hardware components – 4 days
- General IT training – 1 days

Please note:

- Engineers will be involved in solution preparation for FAT providing on-the job training in addition.
- RSD is responsible to nominate qualified staff for the training.
- Travel expenses, which include flights, accommodation and catering for technical team of RSD travelling to Roding, Germany will be borne by RSD.
- Maximum number of participants shall not more than 3.

3.1.7 Training for customer at Mühlbauer Facility

Mühlbauer 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 International Airport site, Mühlbauer provides the following training courses in Roding, Germany to customer team:

- Solution Overview & Solution Operation (1 day)
- Basic Maintenance & Troubleshooting (1 day)
- User manuals and technical documentation will be provided to the customer

Please Note:

- Customer is responsible to nominate qualified staff for the training.
- Maximum number of customer's participants shall be up to 2.
- Travel and accommodation costs for up to 2 customer's participants are included.

3.1.8 Factory Acceptance Test (FAT)

A Factory Acceptance Test (FAT) is a major project milestone and attended by Mühlbauer, and 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.

Please note:

- Travel and accommodation costs for 2 of the customer's participants are included.

3.1.9 Initial Spare Parts Package

Mühlbauer will provide initial spare parts package to customer. List of spare parts will be provided upon delivery. Delivery on the agreed incoterm.

3.1.10 Logistics

The shipment is the essential link between Mühlbauer & Customer, aiming at receiving the deliverables in good conditions, when and where they are needed. This requires a close collaboration between Mühlbauer, customer and the logistic partner.

Mühlbauer responsibility to deliver on **Incoterm CIP Chisinau International Airport**.
From this point **RSD** will take the responsibility to continue the delivery on **Incoterm DDP** to the client address based on the tender requirement.

3.1.11 Installation and commissioning at Chisinau International Airport, Moldova (Entry)

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 is 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.

3.1.11.1 Installation of Main Data Center

RSD is responsible for installation of Main Data Center at its final installation places; after installation RSD has to declare readiness for further installation.

3.1.11.2 Audit of installed Main Data Center

Mühlbauer will provide IT specialists to Audit installed Main Data Center to make sure that it meets pre-agreed specifications and is ready for further project implementation.
Mühlbauer will provide following resources:

- 1x IT Specialist
- 3 days, 8 hours per day

3.1.11.3 Installation of Central and Client system software components

Mühlbauer will provide experienced team on-site in Chisinau International Airport to install Central and Client software components and integrate it to the specified interfaces, including integration with the IGPF infrastructure. Mühlbauer team will be supported by RSD trained engineers.

3.1.11.4 Installation of 5x e-Gates at the Entry (Chisinau International Airport in Moldova)

Mühlbauer team will install 5x e-Gates at the Entry at its final installation place and prepare for further testing and acceptance. Mühlbauer team will be supported by RSD trained engineers.

- 1x Service Technician
- 3 days, 8 hours per day

3.1.12 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 International Airport site, RSD shall train nominated staff at airport for:

- Solution Operation
- Maintenance & Troubleshooting
- Solution Administration

This phase is out of scope of Mühlbauer.

3.1.13 Site Acceptance Test (SAT) Entry

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.
The on-site acceptance process includes inspection and testing of the ABC System *inter alia* document capture, biometric capabilities (facial recognition validation), barrier access control, performance testing, etc. All tests will be documented in a test report, which will be submitted to the Beneficiary for validation.
Prior to the execution of the acceptance testing, a test plan and schedule are 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.

- 1x Service Technician
- 1x Software Technician
- 1x IT Specialist
- 1 day, 8 hours per day

3.1.13.1 Customer testing and validation

The customer will be allocated a period of 30 days for testing and validation, during which documentation of all results, including any non-conformities identified will be done.
This phase will be supported by RSD engineers.

3.1.14 Ramp-up Support

If Ramp-up support is needed, it will be provided by a trained RSD engineer and is out of scope of Mühlbauer.

3.1.15 Support for Installation and Commissioning of 5x e-Gates at the Exit (Chisinau International Airport in Moldova)

Installation and commissioning of the resting 5x e-Gates at the Exit will be contingent upon the Beneficiary's formal acceptance of the PoC results. RSD team will be supported by Mühlbauer team.

- 1x Service Technician
- 2 days, 8 hours per day

3.1.16 Site Acceptance Test (SAT) Exit

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 solution. The on-site acceptance process includes inspection and testing of the ABC System *inter alia* document capture, facial recognition validation, barrier access control, etc.
Prior to the execution of the acceptance testing, a test plan and schedule are 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 RSD.
This phase will be performed by RSD engineers and is out of scope of Mühlbauer.

3.1.17 Technical Documentation

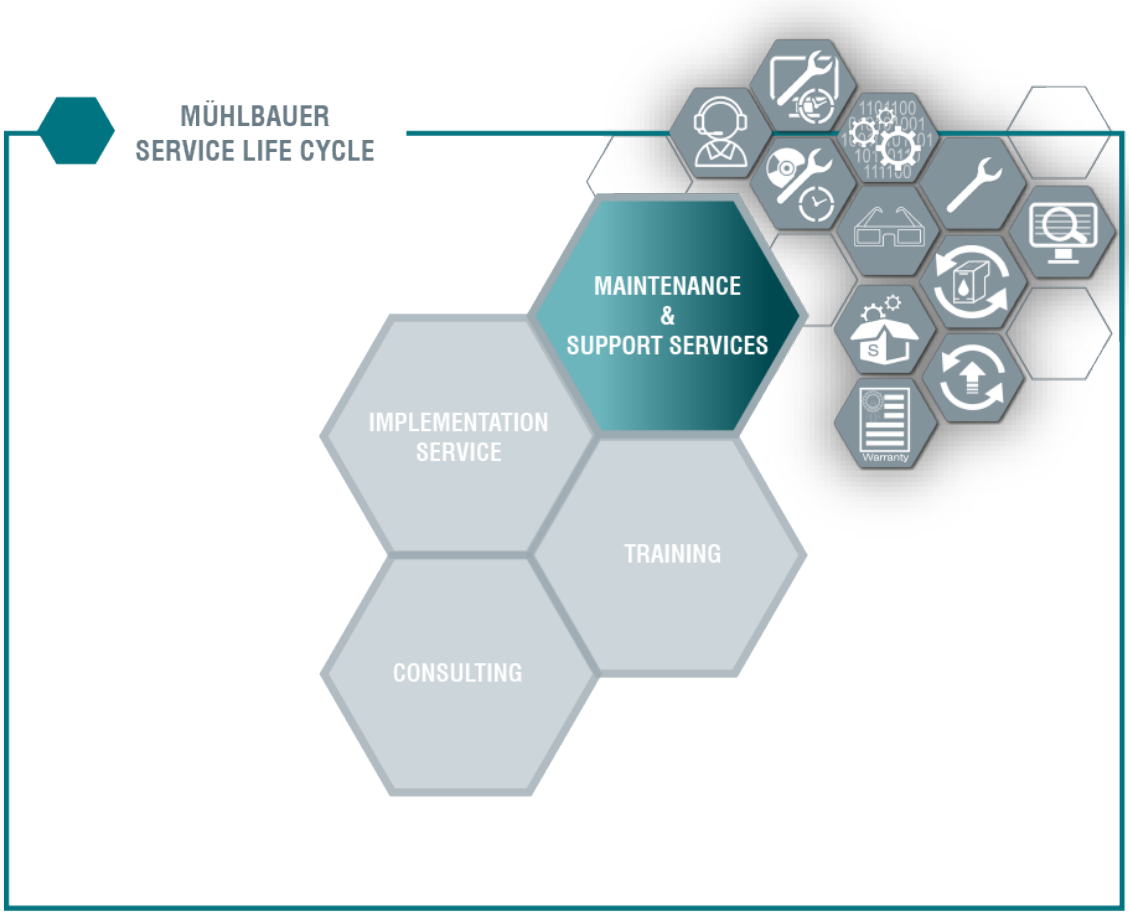
During or upon completion of the implementation (as it will be agreed with the customer), the complete technical documentation as per the tender requirements regarding the system architecture, operational procedures, as well as user manuals and maintenance guides, including detailed plan for preventive and corrective maintenance of the ABC Systems, with indication of regular maintenance intervals and fault diagnosis procedures will be provided. All the documentation will be provided in English and Romanian.

3.1.18 Deliverables for Implementation Service

Pos.	Description	Quantity	Comments
1	**Project Initiation Kick Off Meeting**	1	
2	**Pre-Commissioning at Mühlbauer Facility**	1	Customer to provide interface specification and test interfaces
3	**Training for RSD Engineers in Mühlbauer Facility** • Software Components – 3 days • e-Gate Hardware components – 4 days • General IT training – 1 days		• Engineers will be involved in solution preparation for FAT providing on-the job training in addition. • RSD is responsible to nominate qualified staff for the training. • Travel expenses, which include flights, accommodation and catering for technical team travelling to Roding, Germany will be borne by RSD. • Maximum number of participants shall not more than 3
4	**Factory Acceptance Test (FAT) in Roding**	1	• It is scheduled for 2 days. • Customer is invited to attend the FAT • Travel and accommodation costs for 2 persons of customers FAT delegation are included.
5	**Maintenance & troubleshooting training at Mühlbauer Facility in Germany for** • Solution Overview & Solution Operation (1 day) • Basic Maintenance & troubleshooting (1 day)	1	• Customer to provide adequately skilled staff to receive the training. • Business hours: 8 Hours / day (Mon–Fri) • Travel and accommodation costs for 2 persons are included
6	**Initial Spare Parts Package**	1	
7	**Logistics** All the respective components are delivered to Chisinau International Airport, Republic of Moldova	1	Mühlbauer & Customer will follow: • Agreed Incoterms.
8	**Installation and commissioning at Chisinau International Airport, Republic of Moldova – Entry / Pilot Phase** • 5x e-Gate • e-Gate Software • 3 days in total	1	Customer / RSD is responsible for • Provision of building / facility and its technical prerequisites. • Test data • Test Interfaces • Installation to be supported by RSD trained engineers

9	**Support for Installation and commissioning at Chisinau International Airport, Republic of Moldova - Exit** • 5x e-Gate • e-Gate Software • 2 days in total	1	Customer / RSD is responsible for • Provision of building / facility and its technical prerequisites. • Test data • Test Interfaces • Installation to be performed by RSD trained engineers
10	**Provisional Acceptance Test (SAT) of Entry system:** • 5x e-Gate • e-Gate Software • 1 day	1	Mühlbauer will: • Provide user manuals and technical documentation. Customer will: • Support Mühlbauer during SAT with a technical team who will provide maintenance and support during the contract period. • Provide Operators / staff (to act like Citizens) to enable the workflow test This can be done in agreement with Airport Authorities.

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 ABC System.
Mühlbauer maintenance and support concept can be summarized as below:

3.2.1 Scope of Work for Maintenance & Support

This chapter illustrates high-level break down of Scope of Work for Maintenance & Support between RSD & Mühlbauer during maintenance & Support Phase.

3.2.1.1 Incident Management			
Provision	**Responsible**		**Description**
	MB	**RSD**	
On site and First Level Support		**X**	• Provision of On Site and First Level Support for all technical items according to the tender requirement: - Response time by phone – up to 2 business hours; - Response time for diagnosing the equipment and determining the cause of the malfunction, including remotely (as applicable) – up to 8 business hours; - Response time for restoring equipment functionality, including using spare parts available in stock – up to 3 calendar days; - Response time for restoring equipment functionality using spare parts not available in stock – up to 15 calendar days, excluding time spent on customs procedures; Business hours – from 8:00 a.m. to 5:00 p.m. (And in full compliance to support, response and resolution times requirements of the tender), according to the time zone of the Republic of Moldova. Calendar days – according to the official calendar of the Republic of Moldova. - In the event that a major fault is identified that affects the normal operation of the ABC System, the Bidder must intervene to remedy the fault within a timeframe established in the support agreement, typically no more than 72 hours
Second Level Support		**X**	• Local partner is forming a team of specialists capable of resolving deeper and more extensive incidents in relation to: - Automated Border Control Systems; - Application Software; - Server System; - Network; - Any Facility Components. • Only when this team is no longer able to solve an incident on the Automated Border Control Systems and Application Software the local partner specialist team shall involve the MB specialist team for resolution. Local partner ensures that the tender claim in terms of the required resolution time is met: - Response time by phone – up to 2 business hours; - Response time for diagnosing the equipment and determining the cause of the malfunction, including remotely (as applicable) – up to 8 business hours; - Response time for restoring equipment functionality, including using spare parts available in stock – up to 3 calendar days; - Response time for restoring equipment functionality using spare parts not available in stock – up to 15 calendar days, excluding time spent on customs procedures; Business hours – from 8:00 a.m. to 5:00 p.m. (And in full compliance to support, response and resolution times requirements of the tender), according to the time zone of the Republic of Moldova. Calendar days – according to the official calendar of the Republic of Moldova. - In the event that a major fault is identified that affects the normal operation of the ABC System, the Bidder must

			intervene to remedy the fault within a timeframe established in the support agreement, typically no more than 72 hours
Third Level Support		**X**	• Provision of: - Coordination of any type of 3rd Level Support requirement with the relevant manufacturer; - Remote access to the system if required;
Remote 2nd & 3rd Level Support to RSD for Incident Resolution for 3 years from the date of SAT	**X**		- 2nd & 3rd Level Remote Support over ServiceDesk, Phone, E-mail to RSD Engineers for incident resolution Availability: Mon.-Fri. 08:00-17:00 CET, excluding public holidays in Germany
General Aspects		**X**	• Provide Helpdesk System and Service / Service Staff to enable the announcement of any type of incidence by Email, Telephone, other type of media as a ticket; • Provide incident notice / ticket concerning Application Software, Automated Border Control Systems to Helpdesk System of Mühlbauer; • Maintenance of all incidence to enable tracking of each incidence occurred.
3.2.1.2 Maintenance			
Annual Preventive Maintenance		**X**	Preventive Maintenance for: • ABC e-GATE; (Software & Hardware) done as follows: - Once per year by 1x Hardware Service Engineer for **4 working days** (2 days for entry & 2 days for exit) conducted on site 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 • Check of process stations, such as coding etc. • Check for early detection of defects, replacement of wear parts, minor repairs • Provision of the ongoing training for the end-customer`s technicians throughout the duration of the ABC System's use to ensure its efficient operation and safety
	X		• Once per year for e-Gates Software by software engineer for 3 days conducted on-site

Corrective Maintenance according to needs		**X**	• Providing a team of trained engineers ready to be deployed at the place of installation to conduct corrective maintenance tasks. • To resolve warranty cases within the specified SLA. The local partner ensures compliance with the tender requirements regarding the required resolution time, as follows: - Response time by phone – up to 2 business hours; - Response time for diagnosing the equipment and determining the cause of the malfunction, including remotely (as applicable) – up to 8 business hours; - Response time for restoring equipment functionality, including using spare parts available in stock – up to 3 calendar days; - Response time for restoring equipment functionality using spare parts not available in stock – up to 15 calendar days, excluding time spent on customs procedures; Business hours – from 8:00 a.m. to 5:00 p.m. (And in full compliance to support, response and resolution times requirements of the tender), according to the time zone of the Republic of Moldova. Calendar days – according to the official calendar of the Republic of Moldova. - In the event that a major fault is identified that affects the normal operation of the ABC System, the Bidder must intervene to remedy the fault within a timeframe established in the support agreement, typically no more than 72 hours
Warranty for e-Gates (Spare Parts) for 36 months from the date of SAT	**X**		Spare part for critical issues for 36 months on the term of CIP Chisinau Int. Airport
Warranty & 24/7 technical support for 36 months for IT SW & IT HW for Main & DR Centers		**X**	Warranty and 24/7 technical support for a minimum of 36 months for: - Components of IT systems and network infrastructure—monitoring stations, IT and communications infrastructure (hardware) associated with the ABC system—IT&C equipment necessary for operation - Backup solution - HSM In full compliance with requirements according to Annex 3 of Technical Specification of the Tender
Local Logistics in Moldova		**X**	Customs clearance & Local Logistics and distribution and storage of Spare Parts is in the scope of RSD Storage of emergency spare parts; warranty parts and damaged parts for warranty part exchange

3.2.2 Remote support from Mühlbauer

When it comes to Incident Management Mühlbauer handles the incidents using the following support levels sequentially.

- Mühlbauer 2nd Level Support Specialist Support Group (SSG)
- Mühlbauer 3rd Level Support Research and Development (R&D)

3.2.2.1 Mühlbauer 2nd Level Support (Remote Support)

If RSD team is not able to solve the incident, it is escalated to the Mühlbauer 2nd Level Support team. The 2nd 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.

3.2.2.2 Mühlbauer 3rd Level Support (Remote Support)

If the 2nd Level Support efforts could not solve the incident, it is escalated to the Mühlbauer 3rd 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.

With this package, a full access to Mühlbauer's expertise in providing remote support is included.

3.2.3 Preventive Maintenance for 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 Preventive Maintenance by Mühlbauer engineers periodically to keep the production in top condition. Preventive Maintenance of following will be provided once per year:

- Software Solution (on site) during 3 days
- Access to the system shall be provided by RSD in agreement with respective authority

3.2.4 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 requests)
- Security patches for operating systems if applicable

Please note before applying software updates respective backups are to be taken to make sure restore point in case of malfunction caused by update.
A rollback/recovery plan shall be prepared prior to any software update activity to ensure restoration of the previous stable system state in case of unsuccessful update implementation or unexpected system behavior. The rollback procedure includes validated backup restoration steps, configuration recovery and service verification activities to minimize operational impact and system downtime.

3.2.5 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 for 36 months from the date of Site Acceptance Test. RSD is responsible for replacement warranty parts on the e-Gates.

3.2.6 Deliverables for Maintenance, Support, and warranty

Pos.	Description	Quantity	Comments

1	**Remote support**
	• Mühlbauer remote 2nd and 3rd Level support for:
	  ○ e-Gate(s)
	  ○ e-Gate Software
		36 months	5 days a week. 8-5pm (CET)
			
			Excluding public holidays in Germany

2	**Software Preventive Maintenance** • Once per year for e-Gates Software by software engineer for 3 days conducted on-site	Once per year	Access to the system shall be provided by RSD / Customer.
3	**Warranty - Supply of Spare Parts**	36 months	RSD & Mühlbauer shall discharge their responsibilities as per agreed Incoterms.

For and on behalf of **RSD**

I.C.S. «RELIABLE SOLUTIONS DISTRIBUTOR» S.R.L. 1010600010328

Mr. **Vitalie Birsan**
Administrator

For and on behalf of **Mühlbauer ID Services GmbH**

Mühlbauer
HighTech International
Mühlbauer ID Services GmbH
Josef-Mühlbauer-Platz 1
93426 Roding, Germany
Phone: +49 9461 952-0
Fax: +49 9461 952-1101
Email: info@muehlbauer.de
Internet: www.muehlbauer.de

Mr. **Karl Brandl**
Managing Director

Appendix 1 - Technical Description of the IT&C Infrastructure

Nr. d/o	Denumirea bunurilor solicitate	Specificarea tehnică deplină solicitată, Standarde de referință	Specificarea tehnică ofertata deplină solicitată, Standarde de referință

1	Sistem Storage All-Flash NVMe - 1 bucată	• Echipament nou, neutilizat, nerecondiționat, aflat în producție a ctivă la data livrării
		• Tehnologie All-Flash NVMe end-to-end
		• Controlere redundante active-active
		• Cache total instalat minim 256 GB
		• Capacitate utilizabilă minim 25 TB usable după configurarea unui mecanism de protecție la defect dual (RAID 6 sau echivalent tehnologic distribuit)
		• Minim 4 porturi 10/25Gb SFP+ pentru conectivitate host
		• Suport iSCSI și/sau Fibre Channel
		• Suport multipathing (ALUA sau echivalent)
		• Thin Provisioning
		• Snapshot-uri locale
		• Replicare sincrona și/sau asincrona
		• Compresie și deduplicare inline
		• Criptare date la nivel de disc (encryption at rest)
		• Alimentare redundantă hot-plug
		• Montaj rack 19” inclus
		• Suport tehnic 24/7 minim 36 luni
		• Cerințe de performanță
		• Sistemul trebuie să susțină minim 250.000 IOPS
		• Workload 70% Read / 30% Write
		• Block size 4KB
		• Throughput minim 975 MiB/s la 250.000 IOPS
		• Latență medie totală ≤ 1,0 ms la 250.000 IOPS
		• Grad de utilizare controlere (utilizare CPU) ≤ 65% la 250.000 IOPS
		• Grad de utilizare module NVMe: <55% la 250000 IOPS
		• Performanța declarată trebuie menținută cu mecanism de protecț ie dual activ
		• Sistemul de stocare propus trebuie sa ofere, posibilitatea de identificare a anomaliilor (atacuri de tip ransomwere) online atat pentru operatiunile de citire cat si pentru cele de scrie re. Functionalitate de detectie anomaliilor (atacuri de tip ransom were) trebuie sa ruleze in interiorul echipamentului ofertat si tre buie inclusa in configuratia propusa.
		• Sistemul de stocare propus trebuie sa includa posibilitatea de configurarea de copii imutabile pentru g rupuri de volume, pentru protectia in cazul atacurilor de tip ransomewere. Aceasta functionalitate trebuie sa fie inclusa in configuratia propusa si licentiata corespunzator.
		• Sistemul trebuie să permită scalare peste 300.000 IOPS fără înlocuirea controlerelor
			1x IBM Storage FlashSystem 5300 Control Enclosure
			• Echipament nou, neutilizat, nerecondiționat, aflat în producție activă la livrare
			• Sistem de stocare All-Flash NVMe end-to-end
			• Controlere redundante active-active
			• Cache total instalat: 256 GB
			• Capacitate brută instalată: 6 × 9.6 TB FlashCore Modules (FCM)
			• Capacitate utilizabilă ≥25 TB după configurare DRAID6 (RAID 6 / echivalent distribuit)
			• Conectivitate host:
			  ○ 4 × 32Gb Fibre Channel
			  ○ 4 × 10/25GbE SFP+
			• Suport protocoale: iSCSI și Fibre Channel
			• Suport multipathing: ALUA (sau echivalent)
			• Funcționalități:
			  ○ Thin Provisioning
			  ○ Snapshot-uri locale
			  ○ Replicare sincronă și asincronă
			  ○ Compresie și deduplicare inline
			  ○ Criptare date la nivel de disc (encryption at rest)
			• Alimentare redundantă hot-plug
			• Montaj rack 19” inclus
			• Suport tehnic 24/7 pentru 36 luni
			• Performanță:
			  ○ Performanță susținută: ≥250.000 IOPS
			  ○ Workload: 70% Read / 30% Write
			  ○ Block size: 4KB
			  ○ Throughput: ≥975 MiB/s la 250.000 IOPS
			  ○ Latență medie: ≤1.0 ms la 250.000 IOPS
			  ○ Grad utilizare controlere: ≤65% la 250.000 IOPS
			  ○ Grad utilizare NVMe: ≤55% la 250.000 IOPS
			  ○ Performanța este menținută în configurație redundantă activă
			• Securitate
			  ○ Detecție anomalii (inclusiv ransomware) la nivel sistem
			  ○ Suport pentru copii imutabile (immutable snapshots / safeguarded copies)
			  ○ Toate funcționalitățile menționate sunt incluse și licențiate în configurația ofertată
			• Sistemul permite scalare peste 300.000 IOPS (ex.: 302.655 IOPS conform modelării, cu latență ~1.32 ms) fără înlocuirea controlerelor

1.1	Sistem Backup pe Bandă (Tape Library) - - 1 bucată	**Librărie de benzi modulară**
		• Echipament nou, neutilizat, nerecondiționate aflat în producție a ctivă la momentul ofertării.
		• Arhitectură modulară, scalabilă, care permite extinderea de la unitatea de bază cu minimum 14 module de expansiune.
		• Capacitate de scalare până la minimum 600 de casete.
		• Suport pentru minimum 15 unități LTO Full Height sau minimum 40 unități LTO Half Height.
		• Configurația ofertată trebuie să includă minimum 2 unități LTO-9 Half Height cu interfață Fibre Channel.
		• Configurația ofertată trebuie să includă minimum 40 de sloturi pentru casete.
		• Configurația trebuie să includă minimum 10 casete LTO-9 cu capacitate de minimum 18 TB nativ fiecare (fără compresie).
		• Capacitatea totală livrată trebuie să asigure minimum 180 TB nativ (fără compresie).
		• Casetele trebuie livrate cu etichete cu coduri de bare compatibile cu sistemul de inventariere al librăriei.
		• Configurația trebuie să includă minimum 1 casetă de curățare compatibilă LTO-9.
		• Configurația trebuie să includă minimum 2 surse de alimentare redundante, hot-plug.
		• Echipamentul trebuie să permită definirea de librării virtuale pe ntru fiecare drive instalat.
			1x TS4300 Tape Library Base Module
			• Echipament nou, neutilizat, nerecondiționat, aflat în producție activă la momentul ofertării
			• Arhitectură modulară, scalabilă, cu posibilitate de extindere până la 16 module (1 bază + 15 expansiuni)
			• Capacitate de scalare până la 640 de casete
			• Suport pentru unități LTO Full Height și Half Height
			• Suport pentru până la 16 unități LTO Full Height sau până la 48 unități Half Height
			• Configurația include:
			  ○ 2 × unități LTO-9 Half Height cu interfață Fibre Channel
			  ○ 40 sloturi pentru casete (modul bază)
			  ○ 10 casete LTO-9, capacitate 18 TB nativ fiecare
			  ○ Capacitate totală livrată 180 TB (fără compresie)
			  ○ Casetele livrate cu etichete cod de bare compatibile cu sistemul de inventariere
			  ○ Include 2 casete de curățare compatibilă LTO
			  ○ Surse de alimentare redundante, hot-swap
			  ○ Suport pentru definirea de librării logice (virtual libraries) – până la 21
			• Suport prin licențiere suplimentară pentru funcții:
			  ○ Path Failover
			  ○ Data Path Failover
			  ○ Library Managed Encryption

		• Soluția trebuie să permită activarea, prin licențiere suplimentară, a funcțiilor Path Failover și Library Managed Encryption.
		• Panou frontal pentru operare locală și diagnostic.
		• Minimum 1 port Ethernet 10/100/1000 Mbps pentru management prin interfață Web GUI.
		• Minimum 1 port USB pentru service sau operațiuni locale.
		• Montaj rack 19”.
		• Kit de montare în rack inclus.
		• Sistemul trebuie să fie compatibil cu soluții enterprise de backup pentru medii virtuale și fizice.
		• Suport pentru conectivitate Fibre Channel către infrastructura de servere.
		• Garanție și suport tehnic 24/7 pentru minimum 36 luni.
		
		Cerință de interoperabilitate și suport unificat
		Se solicită ca sistemul de storage principal și sistemul de backup pe bandă să fie produse de același producător sau să fie livrate sub aceeași marcă comercială, în vederea asigurării interoperabilității c ertificate,
		a unui suport tehnic unificat și a unei responsabilități unice privind service-ul și mentenanța.
			• Panou frontal pentru operare locală și diagnostic
			• Interfață de management:
			  ○ 1 × port Ethernet 10/100/1000 Mbps
			  ○ interfață Web GUI pentru administrare
			  ○ 1 port USB pentru service sau operațiuni locale
			• Montaj rack 19”
			• Kit de montare în rack inclus
			• Compatibilitate cu soluții enterprise de backup (Veeam, IBM Storage Protect, etc.)
			• Suport pentru conectivitate Fibre Channel către servere
			• Garanție și suport tehnic 24/7 pentru minim 36 luni
			
			Cerință de interoperabilitate și suport unificat
			Sistemul de storage principal și sistemul de backup pe bandă sunt produse de producătorul IBM, asigurînd interoperabilitatea certificată și a unui suport tehnic unificat.

2	Soluție Software Backup Enterprise – On-Premise	• Se solicită furnizarea unei licențe noi, perpetuale, pentru minimum 20 de instanțe protejate. Soluția trebuie să includă suport producție 24/7 pentru minimum 3 ani.
		• Soluția trebuie să fie certificată pentru platforma de virtualizare utilizată și să fie certificată pentru integrare cu sistemul de storage ofertat, precum și cu sistemul de backup pe bandă ofertat.
		• Soluția trebuie să asigure protecția mediilor virtuale, a serverelor fizice și a stațiilor de lucru/PC-urilor.
		• Trebuie să suporte backup full, incremental și diferențial, precum și mecanisme moderne de optimizare a datelor (forever incremental, synthetic full sau echivalent).
		• Soluția trebuie să permită restaurare granulară la nivel de fișier, aplicație, sistem complet (bare metal) și mașină virtuală, inclusiv restaurare instantanee a mașin ilor virtuale direct din backup (Instant Recovery sau echivalent).
		• Exportul automat al backup-urilor către sistemul de backup pe bandă ofertat trebuie să fie suportat nativ, într-o arhitectură disk-to-disk-to-tape (D2D2T), fără utilizarea de aplicații terțe.
		• Soluția trebuie să includă management integrat al librăriei de ba ndă, cu suport pentru job-uri automate de copiere pe bandă și politici de retenție separate pentru medii disk și tape.
		• Trebuie să includă mecanisme integrate de protecție împotriva ransomware, inclusiv verificarea automat ă a integrității backup-urilor, testare automată a restaurării (SureBackup sau echivalent) și sup ort pentru repository-uri imutabile sau echivalent.
		• Administrarea trebuie realizată prin interfață centralizată unică, cu suport pentru roluri și audit al operațiunilor.
		• Soluția trebuie să funcționeze exclusiv on-premise, fără dependență de servicii cloud pentru funcționalitățil e de bază.
			Veeam Data Platform Foundation Universal Perpetual License
			• Licență nouă, perpetuă (Perpetual Universal License), furnizată în 2 pachete de câte 10 instanțe (VUL)
			• Include funcționalități echivalente Enterprise Plus
			• Include suport producție 24/7 pentru **minim 36 luni (3 ani)**
			• Licența permite protecția următoarelor tipuri de workload:
			  ○ mașini virtuale
			  ○ servere fizice
			  ○ stații de lucru
			  ○ agenți pentru aplicații (ex. baze de date, aplicații enterprise)
			• Soluția este certificată pentru principalele platforme de virtualizare și compatibilă cu sistemele de stocare ofertate, precum și cu infrastructura de backup pe bandă
			• Asigură protecția:
			  ○ mediilor virtuale
			  ○ serverelor fizice
			  ○ stațiilor de lucru / PC-uri
			• Suportă tipuri de backup:
			  ○ full
			  ○ incremental
			  ○ diferențial
			  ○ incremental modern optimizat (forever incremental / synthetic full)
			• Permite restaurare granulară la nivel de:
			  ○ fișier
			  ○ aplicație
			  ○ sistem complet (bare-metal)
			  ○ mașini virtuale, inclusiv restaurare instantanee (Instant Recovery)
			• Exportul automat al backup-urilor către sistemul de backup pe bandă este suportat nativ, în arhitectură disk-to-disk-to-tape (D2D2T), fără utilizarea aplicațiilor terțe
			• Include management integrat al librăriilor de bandă:
			  ○ job-uri automate de copiere pe bandă
			  ○ politici de retenție separate pentru disk și tape
			• Include mecanisme de protecție împotriva ransomware:
			  ○ verificare automată a integrității backup-urilor
			  ○ testare automată a restaurării (SureBackup)
			  ○ suport pentru repository-uri imutabile (immutable backups)
			• Administrare realizată prin interfață centralizată unică, cu suport pentru roluri și audit al operațiunilor
			• Soluția funcționează on-premise, fără dependență de servicii cloud pentru funcționalitățile de bază

3	Firewall Next-Generation – 2 bucăți (High Availability)	• Echipamente noi, neutilizate, nerecondiționate. • Appliance hardware dedicat, format rack-mount 19”, înălțime 1U. • Configurare în High Availability Active-Passive. • Minimum 12 porturi GE RJ45 hardware accelerated. • Minimum 2 porturi WAN dedicate GE RJ45. • Minimum 1 port DMZ dedicat. • Minimum 1 port dedicat management. • Minimum 2 porturi dedicate pentru conexiune HA.	**2x FortiGate 120G (High Availability)** • Echipamente noi, neutilizate, appliance hardware dedicat, format rack 19”, 1U • Configurație High Availability Active-Passive, cu suport Active-Active și clustering • Minim 12 porturi GE RJ45 (16 porturi disponibile) • 2x Porturi configurate/dedicate pentru WAN • 1x Port dedicat pentru management • 1x Port configurat/dedicat pentru DMZ

		• Minimum 4 porturi SFP 1G hardware accelerated.
		• Minimum 2 porturi 10G SFP+.
		• Throughput Firewall (UDP, pachet 1518 bytes) minimum 20 Gbps.
		• Firewall latency maximum 5 µs.
		• Throughput IPS minimum 2.5 Gbps.
		• Throughput NGFW minimum 1.5 Gbps.
		• Throughput Threat Protection minimum 1 Gbps.
		• Minimum 1.5 milioane sesiuni concurente.
		• Minimum 50.000 sesiuni noi pe secundă.
		• Suport pentru SSL inspection minimum 1 Gbps.
		• Suport pentru minimum 2000 tuneluri IPsec site-to-site.
		• Suport pentru clustering atât în mod Active-Active, cât și Active-Passive.
		• Suport pentru rutare statică și dinamică (OSPF sau echivalent).
		• Suport pentru VLAN 802.1Q.
		• Alimentare redundantă (1+1).
		• Licența trebuie să includă minim:
		  ○ IPS (Intrusion Prevention System)
		  ○ Antivirus Gateway
		  ○ Web Filtering
		  ○ Application Control
		  ○ SSL Inspection
		  ○ Advanced Threat Protection
		  ○ Anti-Botnet și protecție împotriva comunicațiilor de tip Command & Control (C2).
		  ○ Threat Intelligence actualizat continuu
		  ○ Integrare cu SIEM / Syslog
		  ○ Actualizări automate semnături pe durata licenței
		• Licențe de securitate complete pentru minimum 36 luni
		• Suport tehnic 24/7 pentru minimum 36 luni.
			• 2x Porturi configurate/dedicate pentru High Availability
			• Minim 4 porturi SFP 1G (8 porturi disponibile)
			• Minim 2 porturi 10GE SFP+ (4 porturi disponibile)
			• Firewall throughput ≥20 Gbps (până la 39 Gbps)
			• Latență ≤5 µs (≈3.17 µs)
			• IPS throughput ≥2.5 Gbps (până la 5.3 Gbps)
			• NGFW throughput ≥1.5 Gbps (până la 3.1 Gbps)
			• Threat Protection throughput ≥1 Gbps (până la 2.8 Gbps)
			• Minim 1.5 milioane sesiuni concurente (până la 3 milioane)
			• Minim 50.000 sesiuni noi/sec (până la 140.000)
			• Minim 2000 tuneluri IPsec site-to-site
			• SSL Inspection ≥1 Gbps (până la ~3 Gbps)
			• Suport clustering Active-Active și Active-Passive
			• Rutare statică și dinamică (OSPF sau echivalent)
			• VLAN 802.1Q
			• VPN IPsec și SSL-VPN
			• Alimentare redundantă (1+1)
			• Licență Fortinet Unified Threat Protection (UTP) inclusă, care acoperă:
			  ○ IPS (Intrusion Prevention System)
			  ○ Antivirus Gateway
			  ○ Web Filtering (URL/DNS Filtering)
			  ○ Application Control
			  ○ Advanced Threat Protection
			  ○ Mecanisme Anti-Botnet și protecție C2
			  ○ Threat intelligence actualizat continuu
			  ○ actualizări automate de semnături pe durata licenței
			• Funcționalitățile SSL Inspection și integrare SIEM / Syslog sunt asigurate nativ de platforma FortiGate
			• Licențe de securitate complete pentru 36 luni
			• Suport tehnic 24/7 pentru 36 luni

3.1	Switch Core – 2 bucăți (configurație redundantă tip stack sau echivalent)	• Echipamente noi, neutilizate, nerecondiționate. • Switch administrabil Layer 2 / Layer 3, format rack-mount 19”, înălțime 1U. • Minimum 24 porturi 10/100/1000Base-T RJ45 per echipament. • Minimum 4 porturi 10G SFP+ per echipament. • Capacitate de switching minim 128 Gbps per echipament. • Throughput minim 190 Mpps (full duplex). • Tabel de adrese MAC cu capacitate minim 32.000 de intrări. • Suport pentru minimum 4096 VLAN-uri. • Minimum 16 grupuri de agregare link (LAG). • Suport pentru LACP (IEEE 802.3ad). • Suport pentru protocoalele STP, RSTP și MSTP. • Suport pentru liste de control al accesului (ACL) – minimum 600 reguli. • Suport pentru mecanism de redundanță între două chassis-uri (stack hardware sau mecanism echivalent activ-activ). • Suport pentru rutare statică și inter-VLAN. • Management prin CLI și SNMP. • Montare în rack 19”. • Alimentare 100–240V AC. • Garanție minim 36 luni.	**2x FortiSwitch FS-124F (configurație redundantă)** • Echipamente noi, neutilizate, nerecondiționate • Switch administrabil Layer 2 / Layer 3, format rack 19”, 1U • 24 porturi 10/100/1000Base-T RJ45 per echipament • 4 porturi uplink 10GE SFP+ per echipament • Capacitate de switching minim 128 Gbps • Throughput minim 190 Mpps • Tabel MAC minim 32.000 adrese • Suport pentru minim 4096 VLAN-uri • Minim 16 grupuri de agregare link (LAG) • Suport LACP (IEEE 802.3ad) • Suport STP, RSTP, MSTP • Suport ACL minim 640 reguli • Suport rutare statică și inter-VLAN • Suport mecanisme redundanță (MCLAG / echivalent) • Management prin CLI, Web GUI, SNMP • Integrare FortiLink pentru management centralizat cu firewall • Alimentare 100–240V AC • Garanție minim 36 luni • Licență FortiCare Premium 36 luni inclusă
3.2	Access Switch – 2 bucăți	• Echipamente noi, neutilizate, nerecondiționate. • Switch administrabil Layer 2 / Layer 3, format rack-mount 19”, înălțime 1U. • Minimum 24 porturi 10/100/1000Base-T RJ45 cu suport PoE+. • Suport PoE conform standardului IEEE 802.3at pe toate porturile RJ45. • Buget total PoE minim 370 W per echipament. • Minimum 4 porturi 10G SFP+ pentru uplink. • Capacitate de switching minim 128 Gbps per echipament. • Throughput minim 190 Mpps. • Tabel de adrese MAC cu capacitate minim 32.000 de intrări. • Suport pentru minimum 4096 VLAN-uri. • Suport pentru LACP (IEEE 802.3ad). • Suport pentru protocoalele STP, RSTP și MSTP. • Suport pentru LLDP și LLDP-MED. • Suport pentru QoS (Quality of Service). • Management prin CLI și SNMP. • Montare în rack 19”. • Alimentare 100–240V AC. • Garanție minim 36 luni.	**2x FortiSwitch FS-124F-FPOE** • Echipamente noi, neutilizate, nerecondiționate • Switch administrabil Layer 2 / Layer 3, format rack 19”, 1U • 24 porturi 10/100/1000Base-T RJ45 cu suport PoE+ (802.3af/at) • Buget PoE minim 370 W per echipament • 4 porturi uplink 10GE SFP+ • Capacitate de switching minim 128 Gbps • Throughput minim 190 Mpps • Tabel MAC minim 32.000 adrese • Suport pentru minim 4096 VLAN-uri • Minim 16 grupuri de agregare link (LAG) • Suport LACP (IEEE 802.3ad) • Suport STP, RSTP, MSTP • Suport LLDP și LLDP-MED • Suport QoS • Suport ACL • Suport securitate porturi și control acces (802.1X / MAC-based) • Management prin CLI, Web GUI, SNMP • Integrare FortiLink pentru management centralizat și NAC • Alimentare 100–240V AC

		Cerință de interoperabilitate și suport unificat Se solicită ca firewall-ul și switch-urile să fie produse de același producător sau să fie livrate sub aceeași marcă comercială, în vederea asigurării interoperabilității certificate, unui suport tehnic unificat și a unei responsabilități unice privind service-ul și mentenanța.	• Garanție 36 luni • Licență FortiCare Premium 36 luni inclusă **Cerință de interoperabilitate și suport unificat** Firewall-ul și switch-urile sunt produse de producătorul Fortinet asigurînd interoperabilitatea certificată și a unui suport tehnic unificat.
4	Servere pentru Virtualizare (cluster) – 2 bucăți	• Echipamente noi, neutilizate, nerecondiționate. • Format rack 2U. • Arhitectură x86_64. • 2 procesoare per server. • Minim 16 core per procesor. • Frecvență bază procesor minim 3.0 GHz. • Cache L3 minim 64 MB per procesor. • TDP maxim 200W per procesor. • Memorie minim 256 GB DDR5 RDIMM 5600 MT/s per server. • Suport memorie ECC. • Boot intern redundat RAID1 pe 2 × SSD M.2 enterprise minim 960 GB. • Fără HDD pentru storage local. • Minim 4 porturi 1GbE RJ45. • Minim 2 porturi 10/25GbE SFP28. • Management out-of-band dedicat. • Suport TPM 2.0. • Secure Boot. • Alimentare redundantă hot-plug (1+1) minim 1400W. • Ventilație high-performance pentru configurație dual CPU. • Kit rack inclus. • Garanție minim 36 luni.	**2x Server Dell PowerEdge R7625** • Echipamente noi, neutilizate, în producție activă • Format rack 19”, 2U • Arhitectură x86_64 • 2× Procesoare AMD EPYC 9124, 16 nuclee / 32 thread-uri, frecvență ≥3.0 GHz, cache L3 64 MB, TDP max. 200W • Memorie RAM 256 GB DDR5 RDIMM 5600 MT/s (4×64GB), ECC • Boot redundant: controller BOSS-N1 cu 2× SSD M.2 960GB în RAID 1 • Fără HDD pentru stocare locală • 6× porturi 1GbE RJ45 (OCP + LOM) • 4× porturi 10/25Gb SFP28 (Broadcom 57504 quad) • Management dedicat out-of-band (iDRAC9 Enterprise) • Modul TPM 2.0 • Secure Boot • Alimentare redundantă hot-plug (1+1), 1400W • Ventilatoare high-performance pentru configurație dual CPU • Kit montare rack inclus (rails) • Virtualization - ProxMox -Standard Subscription 3Y • VM - Windows Server 2025 Std licențiat • Garanție 36 luni
4.1	Server Management – 1 bucată	• Echipament nou, neutilizat, nerecondiționat, aflat în producție activă la momentul ofertării. • Format rack 19”, înălțime 1U. • Arhitectură x86_64. • Un procesor cu minimum 16 core-uri / 32 thread-uri. • Frecvență de bază procesor minimum 3.0 GHz. • Memorie cache L3 minimum 64 MB. • TDP maxim 200 W. • Memorie RAM minimum 64 GB DDR5 RDIMM 5600 MT/s, cu suport ECC. • Boot intern redundant configurat RAID 1 pe 2 × SSD M.2 enterprise, minimum 960 GB fiecare. • Fără HDD pentru stocare locală de date. • Minimum 4 porturi 1GbE RJ45. • Minimum 2 porturi 10/25GbE SFP28. • Port dedicat de management out-of-band. • Suport pentru TPM 2.0. • Suport pentru Secure Boot. • Alimentare redundantă hot-plug (1+1), minimum 800 W. • Adaptor Fibre Channel HBA inclus, interfață PCIe, dual-port. • Minimum 2 porturi Fibre Channel 16 Gb/s sau superior. • Compatibilitate cu unități LTO-9 Fibre Channel. • Suport pentru multipathing / MPIO / ALUA. • Include transceivere optice compatibile și cabluri LC-LC necesare pentru conectare. • Configurare pentru conectare redundantă către cele două drive-uri Fibre Channel sau către două fabrici Fibre Channel independente. • Kit de montare în rack inclus. • Garanție minim 36 luni. **Cerință de interoperabilitate și suport unificat** Se solicită ca serverile să fie produse de același producător sau s ă fie livrate sub aceeași marcă comercială, în vederea asigurării i nteroperabilității certificate, a unui suport tehnic unificat și a unei responsabilități unice privi nd service-ul și mentenanța.	**Server Dell PowerEdge R6615** • Echipament nou, neutilizat, în producție activă • Format rack 19”, 1U • Arhitectură x86_64 • Procesor AMD EPYC 9124 • 16 core / 32 thread-uri • Frecvență 3.0 GHz • Cache L3 64 MB • TDP 200W • Memorie RAM 64 GB DDR5 RDIMM 5600 MT/s (2×32GB) • Suport ECC • Boot redundant: controller BOSS-N1 • 2× SSD M.2 960GB în RAID 1 • Fără HDD pentru stocare locală • 4× porturi 1GbE RJ45 (OCP + LOM) • 2× porturi 10/25Gb SFP28 • 2× adaptoare Fibre Channel HBA dual-port 32Gb • Port dedicat management out-of-band (iDRAC9 Enterprise) • Modul TPM 2.0 • Suport Secure Boot • Alimentare redundantă (1+1), hot-plug, 800W • Compatibilitate LTO-9 Fibre Channel • Suport multipathing (MPIO / ALUA) • Configurație pentru conectare redundantă către două fabrici Fibre Channel sau două drive-uri • Kit montare rack inclus (rails) • Garanție 36 luni • Interoperabilitate certificată și suport tehnic unificat **Cerință de interoperabilitate și suport unificat** Serverile sunt produse de producătorul Dell asigurînd interoperabilitatea certificată și a unui suport tehnic unificat.
5	Hardware Security Module (HSM) – High Availability – 2 bucăți	• Echipament nou, neutilizat, nerecondiționate aflat în producție activă la momentul ofertării. • HSM extern de tip appliance, network-attached. • Montaj rack 19”, format 1U. • Implementare în arhitectură High Availability cu minimum 2 unități fizice.	**2x PROTECTSERVER EXTERNAL 3, TOOLKIT PTK** • Echipamente noi, neutilizate, nerecondiționate, aflate în producție la momentul ofertării • HSM extern de tip appliance, network-attached • Montaj rack 19”, format 1U

		• Cluster activ-activ sau activ-pasiv, cu distribuție a încărcării.
		• Sincronizare automată a cheilor între noduri.
		• Failover automat fără întreruperea aplicațiilor.
		• Replicare a cheilor în timp real (RPO = 0).
		• Certificare minim FIPS 140-2 Level 3, valabilă la data ofertării.
		• Certificare PCI HSM v3 sau superior, valabilă la data ofertării.
		• Carcasă cu protecție anti-tamper.
		• Zeroization automată în caz de compromitere fizică.
		• Surse de alimentare redundante, hot-swappable.
		• Suport pentru autentificare pe bază de roluri.
		• Suport pentru mecanism M-of-N (dual control).
		• Suport pentru autentificare multifactor.
		• Generator hardware de numere aleatorii (True RNG).
		• Performanță minimă:
		  ○ RSA 2048 ≥ 1.300 operații/sec;
		  ○ ECC P-256 ≥ 4.000 operații/sec;
		  ○ AES-256 ≥ 1.000 MB/s.
		• Suport pentru PKCS#11, Microsoft CNG/KSP, Java JCE și OpenSSL engine.
		• Suport SNMP.
		• Suport Syslog și integrare cu sisteme SIEM.
		• Audit logging securizat.
		• Export al logurilor către sistem extern.
		• Funcție securizată de Backup/Restore pentru chei.
		• Sincronizare NTP securizată.
		• Suport pentru algoritmi: RSA 2048/3072/4096, ECC P-256 și P-384, AES 128/256, familia SHA-2.
		• Minimum 2 porturi Gigabit Ethernet per unitate.
		• Suport IPv4 și IPv6.
		• Garanție și suport tehnic 24/7 pentru minimum 36 luni.
			• Implementare în arhitectură High Availability cu minimum 2 unități fizice
			• Suport cluster activ-activ sau activ-pasiv, cu distribuție a încărcării
			• Sincronizare automată a cheilor între noduri
			• Failover automat fără întreruperea aplicațiilor
			• Replicare a cheilor în timp real (RPO = 0)
			• Certificare FIPS 140-2 Level 3, valabilă la data ofertării
			• Carcasă cu protecție anti-tamper și mecanisme de securitate fizică
			• Generare hardware de numere aleatorii (True RNG)
			• Suport autentificare pe bază de roluri
			• Suport mecanism M-of-N (dual control)
			• Suport autentificare multifactor
			• Surse de alimentare redundante, hot-swappable (model 3+)
			• Performanță minimă:
			  ○ RSA 2048 ≥ 1300 operații/sec
			  ○ ECC P-256 ≥ 4000 operații/sec
			  ○ AES-256 ≥ 1000 MB/s
			• Suport pentru PKCS#11, Microsoft CNG/KSP, Java JCE/JCA, OpenSSL
			• Suport SNMP
			• Suport Syslog și integrare cu sisteme SIEM
			• Audit logging securizat
			• Export al logurilor către sisteme externe
			• Funcție securizată de backup/restore pentru chei (inclusiv smartcard)
			• Sincronizare NTP securizată
			• Suport algoritmi:
			  ○ RSA 2048/3072/4096
			  ○ ECC P-256 și superior
			  ○ AES 128/256
			  ○ SHA-2 / SHA-3
			• Minimum 2 porturi Gigabit Ethernet per unitate (port bonding)
			• Suport IPv4 și IPv6
			• Management prin interfață grafică (GUI) și acces remote securizat
			• SEH dongleserver ProMAX included
			• Garanție și suport tehnic 24/7 pentru 36 luni

6	Rack 19” – 1 bucată	• Echipament nou, neutilizat, nerecondiționat. • Rack IT standard 19”, cu înălțime minimă 42U. • Adâncime minimă 1000 mm. • Capacitate de încărcare statică minim 800 kg. • Uși față și spate perforate pentru asigurarea ventilației adecvate. • Panouri laterale detașabile, prevăzute cu sistem de blocare. • Șine verticale reglabile pentru montaj echipamente. • Sistem de împământare inclus. • Spațiu dedicat pentru montarea unui PDU vertical 0U. • Set de șuruburi și cage nuts inclus pentru montajul echipamentelor. • Organizatoare verticale pentru cabluri incluse, minimum 2 bucăți. • Organizatoare orizontale pentru cabluri 1U incluse, minimum 3 bucăți. • Compatibilitate cu echipamente rack 19”. • Patch Panel inclus: • Minimum 2 bucăți patch panel Cat6, 24 porturi fiecare. • Montaj rack 19”, format 1U. • Contacte placate cu aur, minimum 50µ. • Compatibilitate cu cablare Cat6 UTP sau STP. • Suport pentru numerotare și etichetare a porturilor. • Bară suport pentru cabluri inclusă.	**1x 19” Rack-Mount 42U/600*1000** • Echipament nou, neutilizat, nerecondiționat. • Rack IT standard 19”, cu înălțime minimă 42U. • Adâncime minimă 1000 mm. • Capacitate de încărcare statică 800 kg. • Uși față și spate perforate pentru asigurarea ventilației adecvate. • Panouri laterale detașabile, prevăzute cu sistem de blocare. • Șine verticale reglabile pentru montaj echipamente. • Sistem de împământare inclus. • Spațiu dedicat pentru montarea unui PDU vertical 0U. • Set de șuruburi și cage nuts inclus pentru montajul echipamentelor. • Organizatoare verticale pentru cabluri incluse, 2 bucăți. • Organizatoare orizontale pentru cabluri 1U incluse, 3 bucăți. • Compatibilitate cu echipamente rack 19”. • Patch Panel inclus: • 2 bucăți patch panel Cat6, 24 porturi fiecare. • Montaj rack 19”, format 1U. • Contacte placate cu aur, minimum 50µ. • Compatibilitate cu cablare Cat6 UTP sau STP. • Suport pentru numerotare și etichetare a porturilor. • Bară suport pentru cabluri inclusă.
	PDU Rack 0U – 2 bucăți	• Echipamente noi, neutilizate, nerecondiționate. • Unitate de distribuție a alimentării (Rack PDU) pentru montaj vertical 0U în rack standard 19”, conform EIA-310. • Construcție industrială robustă din aluminiu sau material echival ent, rezistent mecanic. • Instalare verticală laterală, fără ocuparea spațiului U în rack. • Kit complet de montaj inclus pentru fixare în rack. • Conector de intrare tip IEC C20 sau echivalent.	**2x PDU G4 BA 0U (C20 16A 1P 12xC13,12xC39)** • Echipamente noi, neutilizate, nerecondiționate • Unitate de distribuție a alimentării (Rack PDU) pentru montaj vertical 0U în rack standard 19” • Construcție industrială robustă din aluminiu, rezistent mecanic • Instalare verticală laterală, fără ocuparea spațiului U în rack • Kit complet de montaj inclus pentru fixare în rack • Conector de intrare tip IEC C20

		• Tensiune nominală 200–240 V AC. • Curent nominal minim 16 A. • Putere nominală minim 3,7 kW. • Alimentare monofazică. • Frecvență 50/60 Hz. • Cablu de alimentare inclus, cu lungime minimă de 3 metri. • Număr total de prize minim 24. • Configurație prize: minimum 12 × IEC C13 și 12 × IEC C19 sau echivalent compatibil. • Prize cu împământare. • Prize prevăzute cu sistem de retenție mecanică pentru prevenire a deconectării accidentale. • Marcaj clar al circuitelor sau al băncilor de prize. • Temperatură de operare minim 0°C – 60°C. • Conformitate CE. • Conformitate cu standardul IEC 62368-1 sau echivalent. • Conformitate RoHS. • Garanție minim 36 luni.	• Tensiune nominală 200–240V AC • Curent nominal 16A • Putere nominală minim 3.7 kW • Alimentare monofazică • Frecvență 50/60 Hz • Cablu de alimentare inclus, lungime 3 m • Număr total de prize minim 24 • Configurație prize: 12 × IEC C13 și 12 × IEC C39 • Design cu prize C39 compatibile atât cu C13 cât și C19 • Prize cu împământare • Prize prevăzute cu sistem de retenție mecanică pentru prevenirea deconectării accidentale • Marcaj clar al circuitelor și al băncilor de prize • Temperatură de operare minim 0°C – 60°C • Conformitate CE • Conformitate standard IEC 62368-1 • Conformitate RoHS • Distribuție optimizată a sarcinii prin bănci de prize colorate • Garanție 36 luni
	UPS Online cu Extensie Baterii (2 seturi)	• Echipamente noi, neutilizate, nerecondiționate. • Se solicită furnizarea unui sistem UPS online dublă conversie (VFI conform IEC 62040-3), destinat utilizării în infrastructuri IT critice, cu putere nominală minim 5000 VA / minim 5000 W și autonomie minim 16 minute la sarcină de 5000 W. Echipamentul trebuie să fie în format rack-mount 19”, cu înălțime maximă 3U pentru unitatea UPS și un modul de baterii externe dedicat 3U, kit de montare inclus și posibilitate de instalare rack/tower. • UPS-ul trebuie să furnizeze undă sinusoidală pură, timp de transfer 0 ms (tehnologie online), tensiune de ieșire reglabilă 200–240V și bypass automat intern. Eficiența în mod online trebuie să fie minim 96.5%. • Sistemul trebuie să fie compatibil cu module baterii externe dedicate, cu posibilitate de conectare a minimum 10 module externe compatibile cu UPS-ul si detectarea lor automata de către acesta la conectare. Modulele de baterii trebuie să fie hot-swappable și gestionate prin sistem inteligent de management al bateriei. Autonomia trebuie să fie extensibilă prin adăugarea de module suplimentare. • Echipamentul trebuie să includă display LCD pentru monitorizare locală, port USB și port serial, precum și slot pentru card de rețea SNMP inclusiv si cardul de reatea pentru monitorizare si control de la distanta a starii UPS-ului prin Fast Ethernet 10/100/1000BaseT. Se solicită suport pentru SNMP v3 și integrare cu platforme de virtualizare (VMware / Hyper-V/Proxmox) pentru shutdown controlat. Certificat de conformitate Cyber Security (IEC 62443-2) • UPS-ul trebuie să fie echipat cu terminal block pentru conexiune, precum și cu minimum 2 prize C19 și minimum 8 prize C13, organizate în cel puțin 2 grupuri controlabile independent (load segments controlate). • UPS-ul trebuie să includă protecție la suprasarcină și scurtcircuit, test automat al bateriilor, MTBF ridicat, garanție minim 3 ani pentru unitatea UPS, cu posibilitatea de prelungire din partea producătorului la expirarea perioadei de garanție, și minim 2 ani pentru baterii. Conformitatea cu standardele IEC 62040-1, IEC 62040-2 și IEC 62040-3 este obligatorie.	**2x Eaton 9SX 5000i RT3U G2** cu extensie **Eaton 9SX EBM 180V RT3U G2** • Echipamente noi, neutilizate, nerecondiționate • UPS online dublă conversie (VFI conform IEC 62040-3) • Putere nominală minim 5000 VA / 5000 W • Format rack-mount 19”, înălțime 3U • Modul baterii externe dedicat 3U, montare rack inclusă • Undă sinusoidală pură • Timp de transfer 0 ms (tehnologie online) • Tensiune de ieșire reglabilă 200–240V • Bypass automat intern • Eficiență în mod online ≥96.5% (până la 96.7%) • Compatibil cu module baterii externe dedicate • Suport pentru conectarea a multiple module baterii (extensibil) • Recunoaștere automată a modulelor baterii • Baterii hot-swappable • Management inteligent baterii (ABM+) • Autonomie ≥16 minute la sarcină 5000W (prin utilizarea modulelor EBM) • Display LCD grafic pentru monitorizare locală • Port USB și port serial RS232 • Slot pentru card de rețea (NM3 Gigabit Network Card inclus) • Suport SNMP și integrare cu platforme de virtualizare pentru shutdown controlat • 8 prize C13 și 2 prize C19 disponibile • Organizare prize în grupuri controlabile • Protecție la suprasarcină și scurtcircuit • Test automat al bateriilor • Protecție descărcare profundă baterii • Funcție securizată de shutdown automat pentru sisteme IT • Conformitate standarde IEC 62040-1, IEC 62040-2, IEC 62040-3 • Alimentare 100–240V AC • Montare în rack 19” inclusă • Garanție 36 luni pentru Eaton 9SX Gen2 UPS • Garanție 24 luni pentru baterii
	Consolă KVM Rack 19” – 1 bucată	• Echipament nou, neutilizat, nerecondiționat. • Consolă KVM rack-mount 19”, montaj 1U glisant. • Include tastatură, touchpad și monitor LCD integrate într-un singur modul retractabil. • Minimum 8 porturi pentru conectarea serverelor. • Conectarea serverelor prin cablu Cat5e/Cat6 sau superior. • Distanță suportată între consolă și server de minimum 25 metri. • Monitor LCD cu diagonală minim 19”. • Rezoluție suportată minim 1366 × 768 @ 60 Hz. • Suport OSD (On-Screen Display). • Comutare porturi prin OSD și taste rapide (hotkey). • Suport pentru funcție auto-scan. • Suport pentru conectare hot-plug a serverelor USB.	1x **NetCommander 8-Port Cat5 1U Rack-Mount Console KVM Switch with 19-in. LCD** • Echipament nou, neutilizat, nerecondiționat • Consolă KVM rack-mount 19”, montaj 1U glisant • Include tastatură, touchpad și monitor LCD integrate într-un modul retractabil • 8 porturi pentru conectarea serverelor • Conectarea serverelor prin cablu Cat5e/Cat6 sau superior • Distanță suportată între consolă și server de minimum 25 metri (până la 30 m) • Monitor LCD cu diagonală 19” • Rezoluție suportată minim 1366 × 768 @ 60 Hz • Suport OSD (On-Screen Display)

		• Suport pentru conectare în cascadă (extindere la minimum 128 servere prin echipamente compatibile).
		• Compatibilitate cu servere USB și PS/2.
		• Alimentare 100–240 V AC.
		• Consum maxim aproximativ 30 W.
		• Kit de montare în rack 19” inclus.
		• Setul va include minimum 8 module/adaptoare server pentru conectare USB + VGA la consola KVM.
		• Modulele server vor permite conectarea prin RJ45 (Cat5e/Cat6).
		• Modulele server nu vor necesita alimentare externă (bus-powered).
		• Instalare plug-and-play, fără necesitatea unui software suplimentar.
		• Garanție minim 36 luni
			• Comutare porturi prin OSD și taste rapide (hotkey)
			• Suport funcție auto-scan
			• Suport hot-plug pentru conectarea serverelor USB
			• Suport pentru conectare în cascadă (extindere până la minimum 128 servere)
			• Compatibilitate cu servere USB și PS/2
			• Alimentare 100–240V AC
			• Consum maxim aproximativ 30 W
			• Kit de montare în rack 19” inclus
			• Setul include:
			  ○ 1 × consolă KVM cu LCD 19”
			  ○ 8 × module adaptor server USB + VGA (SIU)
			• Modulele server permit conectarea prin RJ45 (Cat5e/Cat6)
			• Modulele server sunt bus-powered și nu necesită alimentare externă
			• Instalare plug-and-play, fără necesitatea unui software suplimentar
			• Garanție 36 luni

	Stații All-in-One – 6 bucăți	• Tip: AIO (Monoblock)
		• Memorie instalată: 16 GB DDR5
		• Procesor Tip: min. Intel Core i5 sau Ryzen 5;
		• Frecvență de bază (GHz): min. 2,8 GHz;
		• Numărul de nuclee: min. 8
		• Capacitate de stocare: SSD-NVME 512GB
		• Placă de rețea: integrată;
		• viteză: min. 100/1000 Gb Ethernet
		• Placă video: integrată
		• LCD: diagonala ecranului: min. 23.8";
		• rezoluția ecranului: 1920x1080;
		• tehnologia matricei LCD: IPS;
		• suprafața ecranului: mată (Anti-glare);
		• frecvență: min. 60Hz;
		• sursă de alimentare încorporată;
		• culoare: neagră
		• Mouse: Mouse de acelas brand;
		• Obligatoriu, mouse trebuie sa fie din completul AIO
		• Tastatură: standard, USB, Eng/Rus, de acelas brand;
		• Obligatoriu, tastatură trebuie sa fie din completul AIO
		• Sistem de de operare instalat: Windows 11 Pro
		• Garanție: Min. 3 ani
			6x Dell Pro 24 All-in-One Plus QB24250
			• Tip: AIO (Monoblock)
			• Memorie instalată: 16 GB DDR5
			• Procesor: Intel Core Ultra 5 245
			• Frecvență de bază: ≥ 2.8 GHz
			• Număr de nuclee: 14 nuclee
			• Capacitate de stocare: SSD NVMe 512 GB
			• Placă de rețea: integrată
			• Viteză rețea: 1 Gbps Ethernet (RJ-45)
			• Placă video: integrată
			• LCD: diagonală ecranului 23.8”
			• Rezoluția ecranului: 1920 × 1080 (FHD)
			• Tehnologia matricei: IPS
			• Suprafața ecranului: mată (anti-glare)
			• Frecvență: 100 Hz
			• Sursă de alimentare: incorporată
			• Conectivitate:
			  ○ USB 3.2 Gen 2 / Type-C
			  ○ DisplayPort
			  ○ HDMI
			  ○ RJ-45
			  ○ Wi-Fi + Bluetooth integrate
			• Stand reglabil pe înălțime
			• Mouse: inclus, de același brand
			• Tastatură: inclusă, de același brand
			• Sistem de operare instalat: Windows 11 Pro
			• Modul TPM integrat
			• UPS inclus
			• Garanție: 36 luni

	Soluție Antivirus Enterprise cu EDR – minim 30 bucați	• Număr minim 30 endpoint-uri (servere și stații de lucru), cu posibilitatea realocării licențelor între servere și stații de lucr u fără costuri suplimentare pe durata valabilității. • Consolă de management on-premise, instalată în infrastructura beneficiarului. • Management centralizat prin consolă unică de administrare, cu suport multi-rol și audit al operațiunilor. • Durată licență minim 3 ani, cu suport tehnic inclus pe toată perioada. • Protecție antivirus în timp real. • Protecție anti-malware, anti-exploit și anti-ransomware. • Soluția trebuie să includă mecanism de prevenție ransomware prin tehnici de imunizare / protecție a zonelor critice ale sistemu lui (ransomware vaccination sau echivalent). • Tehnologie EDR (Endpoint Detection and Response) inclusă nativ, fără necesitatea unei platforme extern • Monitorizare comportamentală bazată pe analiză euristică și ma chine learning. • Capacitate de izolare automată sau manuală a endpoint-ului compromis din rețea. • Politici de securitate configurabile granular pe grupuri de dispozitive, utilizatori sau roluri. • Actualizări automate ale motorului de scanare, semnăturilor și m odulelor de protecție. • Scanare la acces, scanare la cerere și scanare programată.	**Bitdefender GravityZone Business Security Enterprise** • Licența acoperă minim 30 endpoint-uri (servere și stații de lucru), cu posibilitatea relocării licențelor între servere și stații de lucru fără costuri suplimentare pe durata valabilității • Consolă de management on-premise, instalată în infrastructura beneficiarului • Management centralizat prin consolă unică de administrare, cu suport multi-rol și audit al operațiunilor • Durata licenței 36 luni, cu suport tehnic inclus pe toată perioada • Protecție antivirus în timp real • Protecție anti-malware, anti-exploit și anti-ransomware • Soluția include mecanisme de prevenție ransomware prin analiză comportamentală și machine learning • Tehnologie EDR (Endpoint Detection and Response) inclusă nativ, fără necesitatea unei platforme externe • Monitorizare comportamentală bazată pe analiză euristică și machine learning • Capabilitate de izolare automată sau manuală a endpoint-ului în rețea • Politici de securitate configurabile granular pe grupuri de dispozitive, utilizatori sau roluri • Permite alocarea dinamică a politicilor de securitate • Actualizări automate ale motorului de scanare, semnăturilor și modulelor de protecție

		• Suport pentru sisteme Windows Server, Windows Client și Linux. • Protecție pentru servere virtuale și medii virtualizate. • Capacitate de integrare cu soluții SIEM prin export log (Syslog sau echivalent). • Raportare detaliată, jurnalizare completă a evenimentelor și posi bilitate export audit. • Protecție împotriva atacurilor fileless și script-based. • Suport pentru control dispozitive (Device Control) și protecție web. • Suport pentru actualizare centralizată și distribuție agent prin pu sh din consolă. • Suport tehnic inclus pe toată durata licenței.	• Scanare la acces, scanare la cerere și scanare programată • Suport pentru sisteme Windows Server, Windows Client și Linux • Protecție pentru servere virtuale și medii virtualizate • Capacitate de integrare cu soluții SIEM prin export log (Syslog sau echivalent) • Raportare detaliată și jurnalizare completă a evenimentelor, cu posibilitate export audit • Protecție împotriva atacurilor fileless și script-based • Suport pentru control dispozitive (Device Control) și protecție web • Suport pentru actualizare centralizată și distribuție agent prin push din consolă • Funcționare on-premise, fără dependență de servicii cloud pentru funcționalitățile de bază
	Monitoare 32” QHD – 10 bucăți	• Echipament nou, neutilizat, aflat în producție activă la momentu l ofertării. • Diagonală 31,5” sau echivalent, certificată. • Rezoluție nativă 2560 × 1440 (QHD). • Panou IPS sau tehnologie echivalentă, cu unghiuri largi de vizualizare. • Luminozitate minim 350 cd/m². • Raport de contrast minim 1000:1. • Timp de răspuns maxim 8 ms. • Rată de refresh minim 100 Hz. • Acoperire de culoare minim 99% sRGB. • Conectivitate minimă: • 1 × HDMI 2.0 sau superior; • 1 × DisplayPort 1.2 sau superior. • Port Ethernet RJ-45 integrat. • Suport pentru ajustare pe înălțime, înclinare (tilt), pivot și rotire (swivel). • Montaj VESA 100 × 100. • Consum redus de energie. • Certificări CE și RoHS. • Garanție minim 36 luni.	**10x Dell Pro 32 Plus QHD USB-C Hub Monitor - P3225DE, 80.1cm (31.5")** • Echipament nou, neutilizat, aflat în producție activă la momentul livrării • Diagonală 31,5” • Rezoluție nativă 2560 × 1440 (QHD) • Panou IPS cu unghiuri largi de vizualizare (178°/178°) • Luminozitate 350 cd/m² • Raport de contrast 1000:1 • Timp de răspuns maxim 8 ms (GTG), respectiv 5 ms în mod accelerat • Rată de refresh 100 Hz • Acoperire de culoare 99% sRGB • Conectivitate minimă: 1 × HDMI 2.1 1 × DisplayPort 1.4 sau superior 1 × port Ethernet RJ-45 integrat (1GbE) • Porturi suplimentare: USB-C cu suport video (DisplayPort) și alimentare Hub USB integrat • Suport pentru ajustare pe înălțime, înclinare (tilt), pivot și rotire (swivel) • Montaj VESA 100 × 100 • Consum redus de energie • Conformitate CE și RoHS • Garanție 36 luni
	Display Profesio nal 65” 4K – 2 bucăți	• Echipamente noi, neutilizate, ne-refurbished, nerecondiționate. • Diagonală minim 65”. • Rezoluție minim 4K UHD (3840 × 2160). • Luminozitate minim 400 cd/m². • Panou IPS sau tehnologie echivalentă, cu unghi larg de vizualizare. • Minimum 2 porturi HDMI. • Minimum 1 port DisplayPort sau echivalent. • Funcționare minim 16/7, destinat utilizării profesionale. • Difuzoare integrate. • Suport pentru montare VESA. • Telecomandă inclusă. • Suport pentru control la distanță prin rețea (LAN) sau interfață dedicată (RS-232 sau echivalent). • Posibilitate de pornire/oprire și configurare a parametrilor de la distanță. • Garanție minim 36 luni.	**2x iiyama ProLite TE6513A-B1AG** • Echipament nou, neutilizat, aflat în producție activă, certificări CE, RoHS, REACH • Diagonală: 65” class (64.5”), design thin bezel • Rezoluție 4K UHD (3840 × 2160), oferit: 3840 × 2160, suport 10-bit color (1.07B culori) • Luminozitate: 500 cd/m², senzor lumină ambientală • Panou IPS 178°/178°, anti-glare, anti-bacterial, zero-gap bonding • 2 x porturi 2.0, HDMI output pentru multi-display • 1 × DisplayPort 1.2, USB-C cu DP Alt Mode • Funcționare profesională (16/7), utilizare profesională, design fanless, MTBF 50.000 ore • Difuzoare integrate, 2 × 20W + subwoofer, ieșire audio S/PDIF • Suport montare VESA: 600 × 400, suport OPS PC slot • Telecomandă inclusă, control software • Control la distanță prin LAN sau RS-232, management centralizat DMS • Pornire/oprire și configurare de la distanță, control remote complet, iiControl platform • Funcționalități suplimentare: Android 14, WiFi 6, Bluetooth 5.0, touch 40 puncte, screen sharing wireless, integrare Google EDLA • Garanție 36 luni

Appendix 2 - Preliminary Project Plan