SITA BORDER CONTROL SOLUTION

Proposal for 10 ABC Gates to

State Enterprise 'Chisinau International Airport'

Date: 21st August 2025

Company Name and Contact Information

Company Details

Company	SITA Advanced Travel Solutions Limited
Division	Border Management
Website	www.sita.aero

Contact Details

Contact:	Dmitry Taranko
Title:	Senior Business Development Manager, Border Management Solutions
Mobile:	(+375) 29 603 65 52
Email:	Dmitry.Taranko@sita.aero

Correspondence Address

Address	Level 5, Block A-C, Apex, Forbury Road, Reading, RG1 1AX, United Kingdom

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

SITA, a world leader in biometrics, border control and passenger processing solutions is honoured to submit this technical and commercial offer for a full fledge automated border control solution (ABC Gates, e-Gates) for Chisinau International Airport, with the end user being the Border Police of Moldova.

SITA's Automated Border Control (ABC) eGates allow for live face biometric capture in combination with the authentication of travel documents, physically and digitally. SITA's seamless eGates offer a best-in-class human-machine interaction and a fast passenger-centric user experience. The result is a considerable increase in throughput, eliminating bottlenecks and enhancing capacity and security.

SITA has extensive experience in implementing, deploying, and supporting border control solutions all over the world: from Punta Cana in Mexico, to Rome in Italy, from Aruba to Jamaica, our Biometric and Border Control solutions help Governments, Passengers and Airports to interact in a seamless and secure way on the border control process.

Our portfolio is delivered in a layered framework through the know-how we gained from over 70 years of experience serving the travel industry in 200 countries and over 25 years of experience delivering end to end border management solutions in all 6 continents for more than 70 governments.

The SITA Automated Border Control solution described in this proposal is designed base d on state-of- the-art technology, which provides your border with flexibility, security and a seamless travel experience. The solution is designed for rapid deployment and convenient operations with SITA supporting you every step of the way.

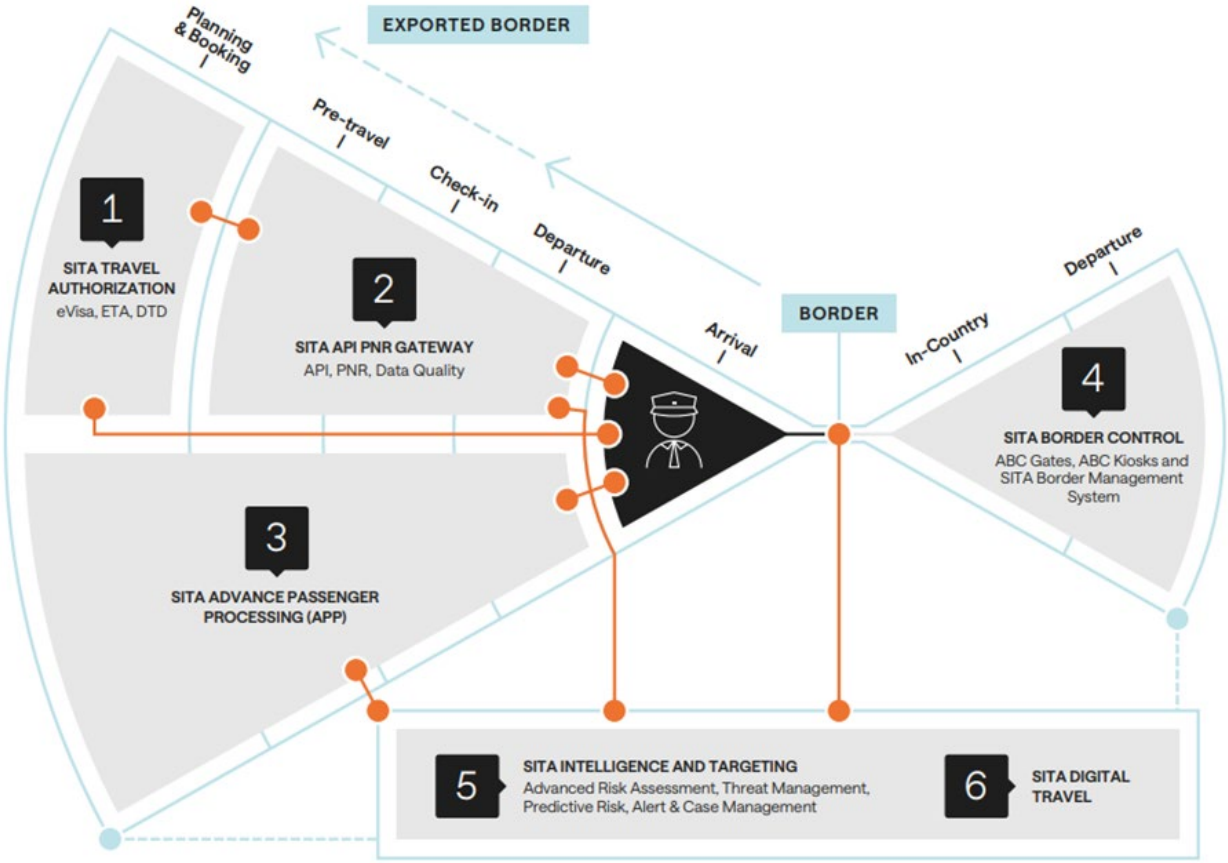
We have a strong track record of successfully implementing similar projects for airport and border control stakeholders worldwide. We have carefully crafted our proposal to address the variables and constraints we anticipate you will encounter, while also ensuring the outcome meets your objectives and requirements.

2. SITA'S BORDER CONTROL VISION

The modern border should provide of a holistic and consistent view of the border across all entry points. There should be a consistent record of individuals entering and leaving your country. Equivalent documentation, risk and identity checks should be performed at all entry points, regardless of the mode of transport. All this information should be underpinned by a central view of all border activity to give you the appropriate information to manage the operation, in real-time.

Today's border needs to apply the appropriate combination of technologies in different situations to deliver these outcomes. It should include a manned capability with all the appropriate devices to clear those travellers that require manual attention.

The modern border should also include a mobile capability to perform ad-hoc checks on travellers or even to process travellers on buses or trains using tablets or mobile phones. Unexpected situations will occur so there should be a means to set up temporary or emergency checkpoints using solutions in suitcases for portability. All these approaches must perform equivalent and appropriate levels of scrutiny on the documentation being presented, the identity verification and the risk assessment of the traveller.



SITA's Border Management Portfolio is the world's only end-to-end offering for Integrated Border Management

These systems must also be integrated with other common types of systems that are used in a border management context. These are typically visa management systems, identity

databases and risk assessment systems. This integration ensures that the Border Guard always has the appropriate information available to make the entry or exit decision.

SITA uses the most effective and appropriate biometric capture technologies and matching algorithms for specific deployments. This enables us to provide accurate and fast identity verification, whilst providing you with the most cost-effective solution.

Through partnerships with industry leading providers, SITA can offer unsurpassed biometric matching algorithms that provide high accuracy and selectivity. The quality and speed of the core technology are validated through a comprehensive range of tests, from small one-to-one verification all the way up to large-scale, high-volume identification matching, conducted by the National Institute of Standards and Technology (NIST) and others.

3. WHAT MAKES SITA'S BORDER CONTROL SOLUTION UNIQUE?

Gateway to Tomorrow: Seamless Security for the Digital Traveller

In today's rapidly evolving travel landscape, the need for robust, efficient border security has never been more critical. Our automated border control solution offers state-of-the-art technology tailored to meet these challenges head-on.

Implementing a modern automated border control gate positions the immigration agencies as leaders in technological innovation, enhancing its reputation as a forward-thinking entity committed to improving security and traveller experience.

This upgrade not only streamlines operations but also visibly demonstrates the agency's commitment to using cutting-edge technology to ensure efficient and secure border management.

Below, we explore the key selling points that set our system apart, highlighting its effectiveness and efficiency in enhancing border security operations.

DTC Ready: Experience the future of travel with our revolutionary automated border control gate. Utilizing state-of-the-art biometric technology, this system is ready to ensure a swift and secure border crossing by supporting the different types of **Digital Travel Credentials (DTC).** As the leaders in Digital Travel, SITA Automated Border Control Gate was developed to support natively Digital Travel Credentials verification and paperless border processes, supporting a more connected cross border travel; Leveraging in the Global Footprint of presence in more than 200 countries and 1000 airports, we are in a unique position to support trans-government information sharing.

Effortless Integration: Engineered for seamless integration with existing border control systems, this advanced solution is built to enhance security and streamline the immigration process, accommodating all standardized protocols and data systems. With its **adaptable technology**, it ensures smooth **interoperability** and swift traveller processing, making it an ideal upgrade for modernizing and connecting to the existing border security systems that are in place.

Engineered for Reliability: Built on a foundation of years of expertise in high-critical and high- availability environments in the Travel industry, our software embodies the pinnacle of reliability and performance. With **70 years of experience** in developing robust solutions for demanding scenarios in the Government, Airlines and Airports ecosystems, we offer software and hardware you can trust implicitly. Our track record of excellence in complex, **mission-critical projects** ensures that our software and hardware not only meet but exceeds the stringent demands of the border operations, providing **reliability when it's needed the most.**

Tomorrow's Design, today: Our automated border control gate features the most modern design on the market, meticulously crafted with the passenger experience at its core. Combining sleek aesthetics with advanced functionality, this gate is engineered to facilitate a smooth, intuitive interaction for every traveller. With its state-of-the-art technology and ergonomic design, it sets new standards in border control efficiency and comfort, ensuring a seamless and positive journey from start to finish.

Face Forward: Unlocking Seamless Travel with a Glance: With decades of pioneering experience in biometric technology, our team has been at the forefront of developing and refining face recognition systems. Our expertise spans a broad array of applications, from

enhancing airport security to streamlining airplane boarding processes. Our advanced algorithms and innovative approaches have set industry standards, ensuring reliable identification and verification through facial recognition. With more than 4000 biometric devices in operation worldwide, we provide biometric solutions you can trust.

4. SITA AUTOMATED BORDER CONTROL GATE

SITA ABC Gates simplifies the border crossing experience for the traveller while at the same time providing governments with the confidence that appropriate security controls are applied meaning that only suitable travellers can cross the border. SITA ABC Gates provides a fully automated, self-service immigration experience for the traveller, using robust documentation checks and biometric identity verification of travellers and are fully compliant with the Frontex specification for Automated Border Controls and future ready for the European Entry-Exit System requirements.

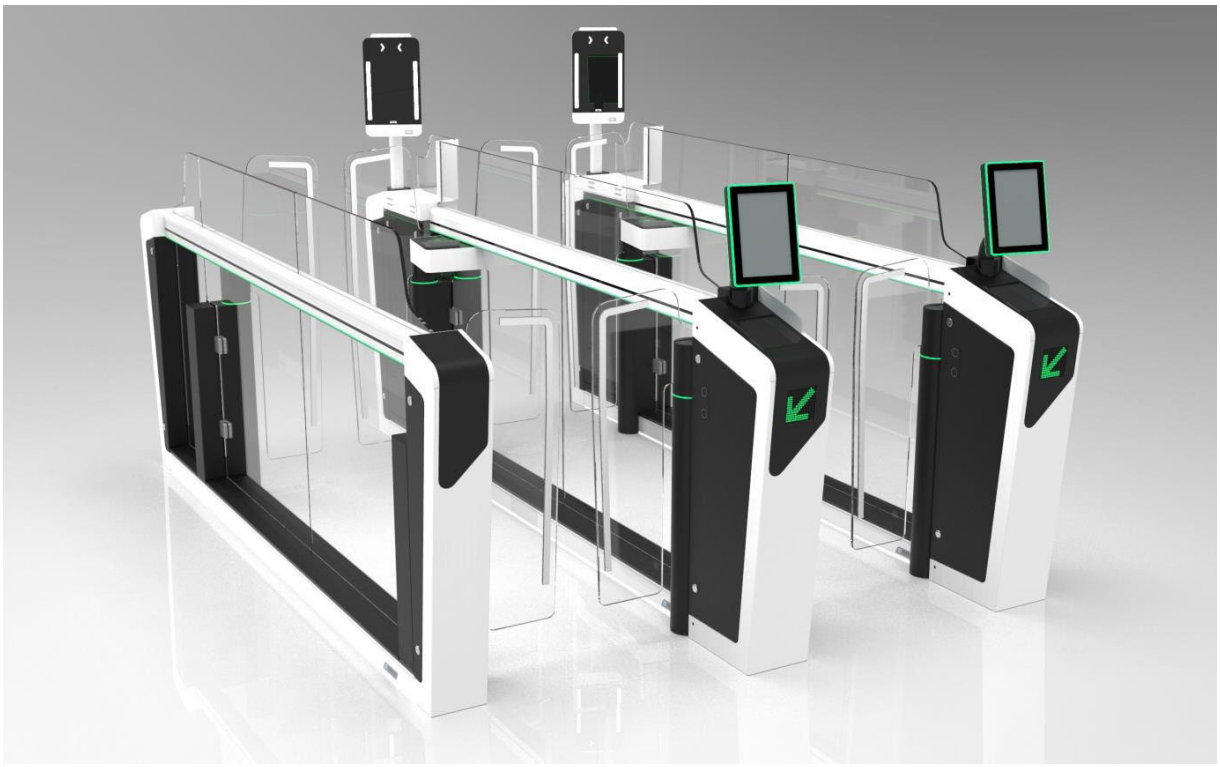


Figure 1 - General view of two SITA ABC Gates

In designing the ABC Gate, a focus on modern and avant-garde aesthetics guided the overall style, featuring integrated forms such as round, thin, and compact elements with flowing lines and surfaces. The design strives for transparency, minimizing the presence of edges, joints, and joints to create a seamless appearance. Clear safety glass is preferred for visibility and integrity. Durability is a key consideration, with vandal-proof principles applied to all components accessible to passengers, alongside the use of scratch-proof materials. For maintenance ease, the main materials can be cleaned with simple methods like soap and cloth. Additionally, the mechanics and components of the gate are fully integrated, ensuring both functionality and sleek design.

- All components, such as motorized mechanisms and biometric readers, are integrated into the eGates structure, forming a completely self-contained unit. This means that there is no need for considerable engineering interventions in the airport to deploy it, because all its components and sensors are embedded in the

eGates structure, leaving only the necessary power and communication interfaces open.

The proposed offer considered the installation of 10 eGates, follows:

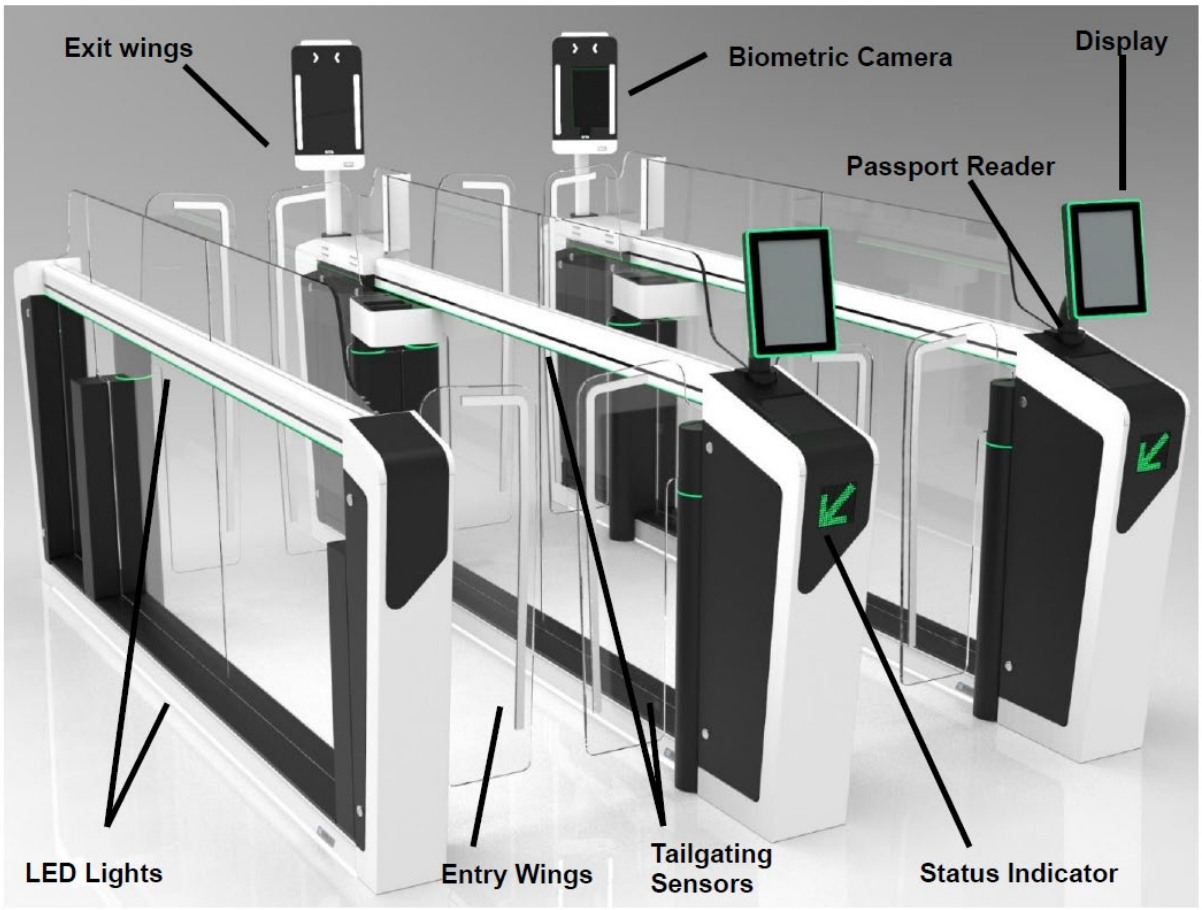
- **Arrivals:** 5 eGates with 1 monitoring station.
- **Departures:** 5 eGates with 1 monitoring station.

This configuration supports balanced traveller flow at arrival and departure points, with real-time supervision through dedicated monitoring stations.

- The eGates allows citizens of the Republic of Moldova who are 18 years or older and are not accompanying minors to cross the state border. The system provides flexibility and technical capability to expand eligibility to additional categories of persons, as determined by the General Inspectorate of the Border Police in accordance with evolving regulations.

Both the hardware and software components within the proposed integrated border management solution are modular and flexible. While the Biometric Engine supports and manages multiple biometric modalities, the eGates hardware is as well composed by several modules, each specialized for its functionality and all together building a border clearance tool, which is optimized for performance, speed and security. It was conceived to allow a fast replacement of devices.

4.1 ABC Gate Components



4.1.1 Biometric Camera

Through partnerships with industry leading providers, SITA can offer unsurpassed biometric matching algorithms that provide high accuracy and selectivity. The quality and speed of the core technology are validated through a comprehensive range of tests, from small one-to-one verification all the way up to large-scale, high-volume identification matching, conducted by the National Institute of Standards and Technology (NIST) and others.

Through partnerships with industry leading providers, SITA can offer unsurpassed biometric matching algorithms that provide high accuracy and selectivity. The quality and speed of the core technology are validated through a comprehensive range of tests, from small one-to-one verification all the way up to large-scale, high- volume identification matching, conducted by the National Institute of Standards and Technology (NIST) and others.

Figure 2 Biometric Capture Device

SITAs Face Pod is a self-identification Biometric solution that offers dynamic facial recognition. It captures a high-quality ICAO Compliant live image of the traveller ’s face and makes it available for biometric matching. The device Pod includes a 10-inch LCD display which presents animations to the traveller on how to progress through the ABC Gate.

It has built in chevron LED that provide extra illumination if required, for high quality face capture, and status LED lights to indicate to traveller s when to proceed and look into the camera.

It features:

- Face capture camera and Lens
- Port RGB LED Controller Board
- Camera status Indicator LEDs
- Internal PC

The SITA face capture algorithm continuously analyses the video stream from the cameras to detect the passenger's face. As soon as a face is detected at the correct distance from the camera, based on the pixels between the eyes, a quality assessment algorithm is run to check if the face image reaches the minimum criteria based on ISO 39794-5 and ISO/IEC 19794-5:2011 Face image (eye distance, blur, focus, pose, expression).

If the quality requirements are not met, the camera's shutter speed is automatically adjusted, based on the brightness of the face, to optimize the capture. This adjustment is a critical part of the process to compensate for difficult lighting conditions such as backlighting or low light. When the face image meets the quality requirements, algorithms can be run to optimize the images (rotate the face to align the ears horizontally, adjust contrast and brightness to optimal settings, adjust white balance). The face image is then cropped to achieve a requirement of a minimum of 120 pixels between the eyes and a minimum of 800 x 600 pixels in size.

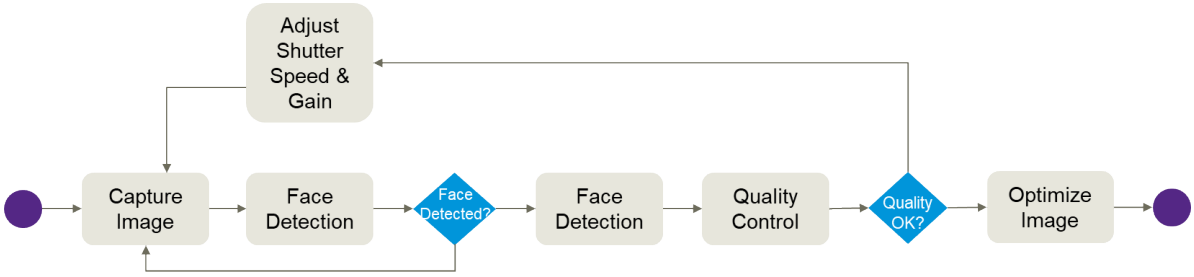


Figure 3 Face Capture Process

4.1.2 Travel Document Reader

The travel document scanner is the first point of contact the SITA ABC Gate has with the traveller. It captures and validates passport data and its authenticity.

It is designed to collect traveller biographic and biometric data and interface with government border control systems. It includes a progress bar to help direct the user during the scan and visually show the result of the scan.

Its flat top and open design with new user instructions makes the scanner area clearly visible and overall creates a more efficient user experience and the anti-glare technology helps reduce laminate reflections and ambient light interference therefore improving image quality.

Figure 4 Travel Document Reader

The SITA ABC Gate application performs the following authenticity checks, using the passport reader:

Optical Controls:

Determination of the document type as specified in the ICAO Best Practice Guidelines for Optical Machine Authentication and Spectrally selective controls, different reactions that occur on a

document illuminated with visual light (white light) or extra-visual illumination (UV, IR) - including controls associated with the type of document, namely:

- Control of MRZ area for ICAO 9303 compliance
- Checking the consistency of the MRZ area using checksums

- Checking that the MRZ area is readable under IR light
- Check that the data in the MRZ area is printed using the OCR-B type face

Electronic Controls:

- Authenticity and consistency checks based on a certification structure:
- EF.SOD verification
- DS Verification of the certificate signature
- DS Certificate of validation of the control period
- DS Certificate revocation status
- Compare EF.SOD vs EF.COM
- Data set integrity check

Comparison of issuing countries (DG1 vs DS Certificate)

Figure 5 White Light

Figure 6 Infra Red Light

Figure 7 Coaxial white light

Figure 8 Ultraviolet Light

These checks are supported by certificate acquisition processes (DS/CSCA and related CRLs for all countries involved) based on integrations that download certificates on a server to perform these checks and applying the appropriate security mechanisms (BAC, PACE, PA, AA, CA, TA).

Combined Checks:

Checks that combine the data read by the OCR from the data page and the data read from the chip are also performed:

- Comparison of issuing countries (DG1 vs DS Certificate)
- Checking the expiry date of the passport (data page, DG1) against the current date
- MRZ optical reading vs electronic biographical data DG1
- Comparison of passport and MRZ visa data (when available)

Whenever possible depending on the type of travel document:

- Compare the data extracted from MRZ with the data extracted from Visual Inspection Zone on the data page
- Check DG2 with the facial image of the VIZ on the data page.
- SITA Document Validation solution will also be provided: in particular, an appropriate library of document templates will be installed in the central system and regularly updated (quarterly) as part of the solution. The document validation software will also be regularly updated to incorporate support for new optical verification templates.

4.1.3 Dimension and Physical Features

The ABC Gates was designed having in mind the structural dimensions tailored to human scale and the aesthetic elements that contribute to a seamless, modern, and secure entry experience. By exploring material choices, mechanical integrations, and design strategies aimed at enhancing durability and ease of maintenance.

The eGates system is delivered as a very robust unit where all core components, including biometric reading devices, document readers and door motors are protected by metallic vandal-proof encasings and panels. Internal devices, such as the power and processing units, as well as all internal fittings and cables are also protected and hidden behind robust metallic panels, in order to prevent them from being accessible and visible to passengers. Thus, the entire system is designed and built so that the damage susceptibility of every component is minimized while allowing for a smooth clearance journey and preventing any kind of injuries to passengers.

The walls are designed to withstand normal use, and the lower section is reinforced to protect from damages when hit by luggage carried by the passenger, such as trolleys. Even so, if the glass brakes due to a strong impact, it shatters completely to avoid serious injuries.

Figure 9 Example of a bank of gates

The chassis creates a light weighted but strong structural element that prevents the eGates from being physically deformed when it suffers strong hits either from passengers or luggage. All eGates modules are mounted on this chassis, which provides the eGates system with an open and modular architecture concept and the possibility to incorporate future upgrades, either by simply inserting more modules, or by exchanging self-contained modules.

The proposed ABC Gates are modularly connected to each other in line, so that the left-hand side of one passage is the right-hand side of the next passage, providing a clean and uniform look to a group of eGates of any size. The modularity reduces the total area of the airport occupied by a row of eGates, when compared to a set of eGates deployed separately, and simplifies the integration of additional eGates.

A wide lane ABC Gate unit can be provided for travellers who need assistance for example, travellers with reduced mobility or travellers carrying large baggage. In this version the passage width is increased to 900 mm.

The physical features of the ABC Gate are summarized bel

- The integrated 7-inch instruction screens display pictures, video and animation instructions to the traveller. The screen designs are simple, employing graphics indicating the next user action with a minimal of accompanying text. Our experience shows that this is the best approach to maintain high throughput.
- Entrance and exit barriers each have a double-door configuration to enable two-stage control.
- The door wings are the fastest available, with opening / closing time of 0.5 sec. for the standard door wings. This improves traveller throughput.
- The door motors contain a smart sensor system to reach the highest level of international security and safety requirements.
- The large glass surfaces provide high visibility to the Border Guard to detect suspicious behaviour inside the secure zone.
- The modular design allows for components to be moved inside or outside the secure zone as needed. For example, the document scanner can be positioned inside the secure zone providing a one-step ABC process.
- The ABC Gates can be installed as single or multiple lanes, sharing common side barriers to optimize physical footprint and cost. Any ABC Gates already installed can be easily extended with additional lanes.
- It provides a user-friendly and ergonomic experience for the traveller. It is intuitive and easy to use.
- The ABC Gates operates on low energy drive to minimize power consumption.
- The MCBF (Mean Cycles Between Failure) is up to 10 million now in a typical immigration environment.
- There are no large horizontal surfaces within the secure zone to avoid situations where travellers accidently leave items behind.
- There is no unnecessary moving parts or heavy-duty lighting

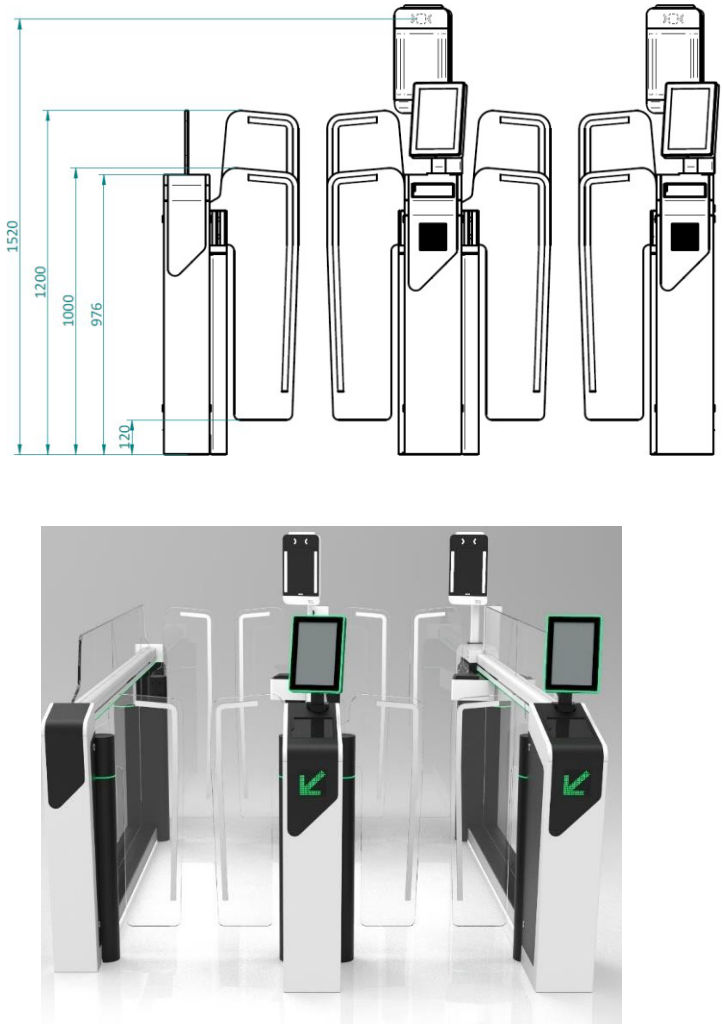


Figure 10 Wings, Housing and Camera Heights

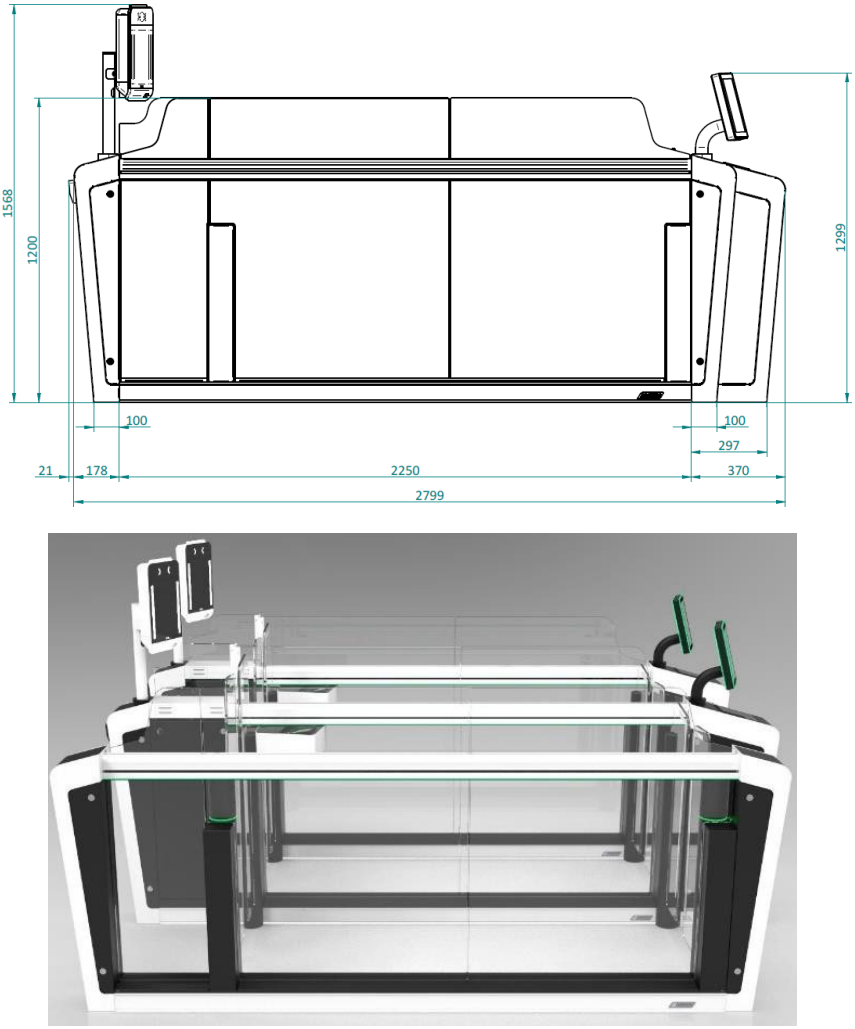


Figure 11 Length, Height & Glass Height

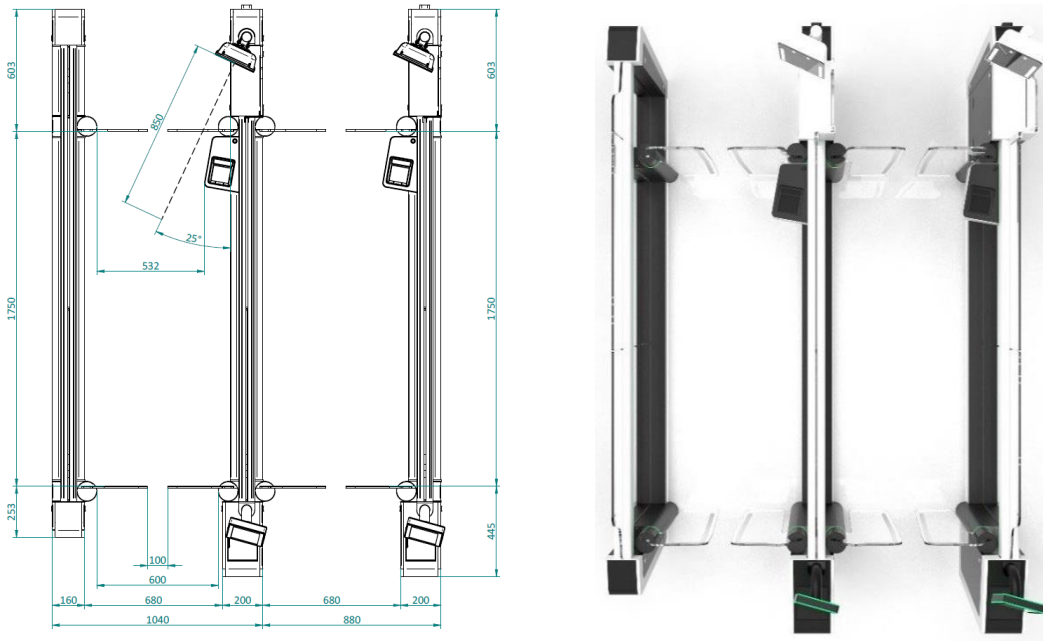


Figure 12 Wings position, Housing Widths, Passage Width

4.1.4 Safety and Security

Each ABC Gate includes sophisticated sensors and an e-Gate Controller that can detect a range of security-related conditions including:

- The ability to differentiate an adult or child walking, plus hand luggage, plus suitcases and bags on wheels (pulling or pushing).
-
- The ability to detect multiple persons (adults or children) entering the secure zone to prevent tailgating, and the inclusion of sensors and features to prevent crossovers during passage through the gates.
- The ability to detect attempted forced opening of the entrance and exit doors.
- The ability to detect a passenger transiting in the wrong direction.
- The ability to detect baggage or other unexpected items left in the lane.
- The ability to detect excessive time taken to pass through the open entrance or exit doors.
- Safety sensors prevent users from being pinched or injured.

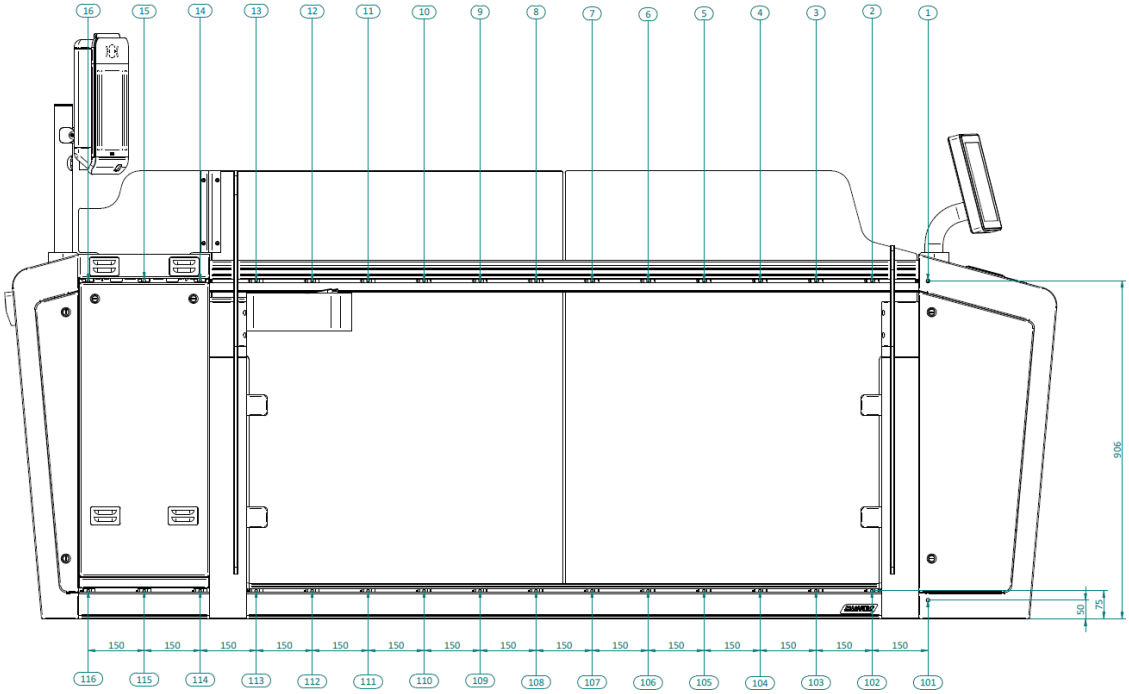


Figure 13 Example of tailgating

Top and bottom of the eGates structure are equipped with our state-of-the-art sensor technology designed specifically for an automated border control process. This cutting-edge system is engineered to detect and alert for any unusual activities or unauthorized access, ensuring maximum security with minimal oversight. In total 36 sensors are collection and analysing in real time information and will provide an alert to the passenger and/or border officer if necessary. Automated border control gates are designed to manage and monitor the entry and exit of individuals across borders. Tailgating, where an unauthorized person follows an authorized individual closely through the gate, poses a significant security risk. Effective tailgating detection prevents unauthorized access, ensuring that only verified individuals can

enter or exit, thus upholding the integrity of a nation's borders. An array of tailgating sensors (indicated in blue in the image above) placed next to the floor and on the top structure of the gate detect tailgating situations.

Another common situation in an automated border control process is where the passenger completes the border process but exit the ABC Gate leaving his luggage behind. In this situation, the ABC gate will keep the exit doors open (allowing the passenger to return to pick up the luggage), while keeping the entry doors closed, to avoid the next passenger to interact with the left luggage.

Figure 14 The ABC Gate is capable of detecting abandoned objects left inside the secure area

4.2 ABC High Level Process

The following sections provides an overview of the proposed workflow of the ABC Gate and software components that will orchestrate and build the state-of-the-art automated border control solution.

The diagram below presents the high-level overview of the eGates activities, and the information exchanged. After project kick-off and during specifications closure phase, a detailed solution scope of works based on the image below will be discussed and agreed with the Chisinau International Airport and Border Police of Moldova.

As part of this project, SITA envisions the following technical responsibilities between SITA system and customer backend system, to be further discussed and agreed after project kick-off.

SITA System will:

- Capture the passenger's biographic data, by reading their electronic Document (Passport);
- Confirm the authenticity of the passenger's Document by performing visual and electronic security validations.
- Determine the passenger's eligibility to use the eGates system based on their Document.

- Capture the passenger's face biometric data and ensure that the face biometric data captured complies with predetermined quality parameters;
- Verify the passenger's identity by performing a face biometric match between the reference data (extracted from the eDocument chip) and the live data.
- Send the passenger's biographic and biometric data, as well as the result of the biometric verification to the customer backend system.
- Wait and process the instruction received from the customer backend system as to the outcome of the transaction.

The Border Police Backend System will:

- Provide a set of the service calls that allow the SITA system to retrieve the clearance status of the passenger as well as send the passengers' data.
- Validate the clearance status of the passenger based on the travel document data. This result will determine if they are allowed to exit the eGates automatically or they required to be further processed by an officer.
- Perform blacklist and watch list validation and send the result to the SITA system;

4.2.1 Automated Border Control Workflow

4.2.1.1. Capture and Validate Travel Document (passport)

- The passenger scans the Document on the eGates document reader.
- The information is validated using the corresponding templates (UV, IR and visible light) and certificates for the digital signature (for ePassport).
- The information is sent to the customer backend system which responses with eligibility of the Document (e.g., watchlist hit, stolen document).
- Passenger enters inside the eGates;

4.2.1.2. Capture and Verify Face

- The eGates captures a live image of the passenger's face.

- The capture is biometrically verified against the image obtained from the eDocument

4.2.1.3. Verify Border Crossing with Backend

- The eGates send all the information to the backend
- The backend allows or rejects the border crossing

As seen above, the transaction workflow can be viewed as two main steps:

- The **first step** is performed before the entry doors, while the passenger is outside the eGates. It is comprised of the Document reading and its validation.
- The **second step** refers to the part of the workflow that occurs while the passenger is in the mantrap area of gate (between entry and exit doors). This step consists of biometric capture, validation and action of the clearance check. Additionally, during this step the eGates is continuously monitored to ensure that only a single passenger is in the eGates.

4.3 Monitoring workstation

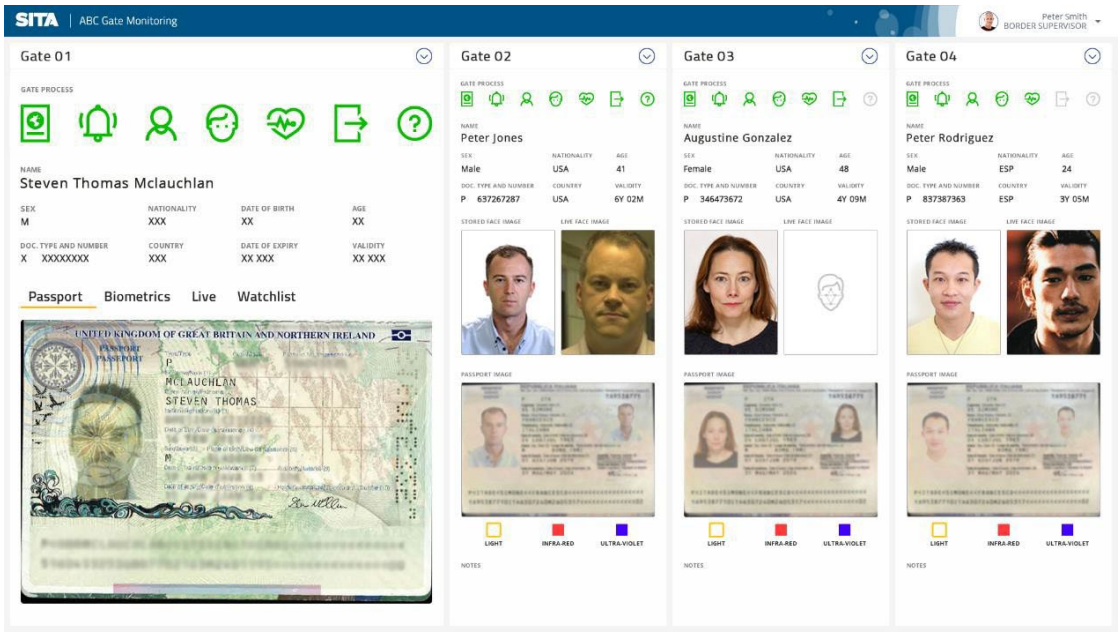
The Monitoring Workstation allows a Border Guard to monitor and control a group of ABC Gates from a single workstation. One monitoring station can allow a Border Guard to view and manage up to six to height gates at one time. The monitoring station will be provided by SITA.

The setup of the ABC Gates in the monitoring console is controlled by a configuration file. In addition, only operators with the required account privileges may use the ABC Gates Monitoring Workstation to activate, deactivate and monitor the ABC Gates.

Each ABC Gate is identified and shown as active or inactive (greyed out). The travellers face image as captured from the travel document or during enrolment and live image from the ABC Gates are shown along with their status (documents verified, biometrics verified, risk status, etc.).

Access to the administration interface and monitoring stations is protected by multi-factor authentication (MFA) and role-based access control (RBAC) policies.

In addition to monitoring the ABC Gates, the Border Guard has full control of the ABC Gate and may open both entry and exit doors (the door will close automatically upon timeout or after the traveller has passed through) reset, reboot and activate or deactivate ABC Gates.



Main Features of the monitoring workstation:

- Visualization of the electronic document data retrieved from the document, including the face image and passenger biographical data.
- Visualization, when required, of the images scanned by the document reader in the natural, infrared, ultra-violet and coaxial wavelengths.
- Visualization of the results of the document verification and authentication tests performed by the document reader device.
- Monitoring and control of the automatic biometric recognition process, including visualization of the live captured images of the passenger and the possibility to perform manual recognition, if necessary.
- Visualization of the results of the biometric recognition procedure. When the score of the biometric recognition falls below the minimum or exceeds the maximum specified value, the application displays alerts.
- Visualization of live video images from the face camera.
- Real-time monitoring of transactions including eGates status, document data, biometric match result and exceptional situations detected.
- Warning of alarm conditions and other notifications (e.g. tailgating, abandoned objects).
- Manual override commands for providing assistance or assuring eGates operation.

Figure 15 Border Officer Supervising eGates in Operation

4.4 System Administration Capabilities

Two different client applications will be provided to meet the needs of different users:

SITA ABC Monitoring application (with customized functionalities for each user role) for System support staff for technical monitoring and control Supervisors to monitor and control the ABC Gate process. "Admin Portal" for dedicated analyst and control roles (business users) to extract process and performance KPIs and create reports.

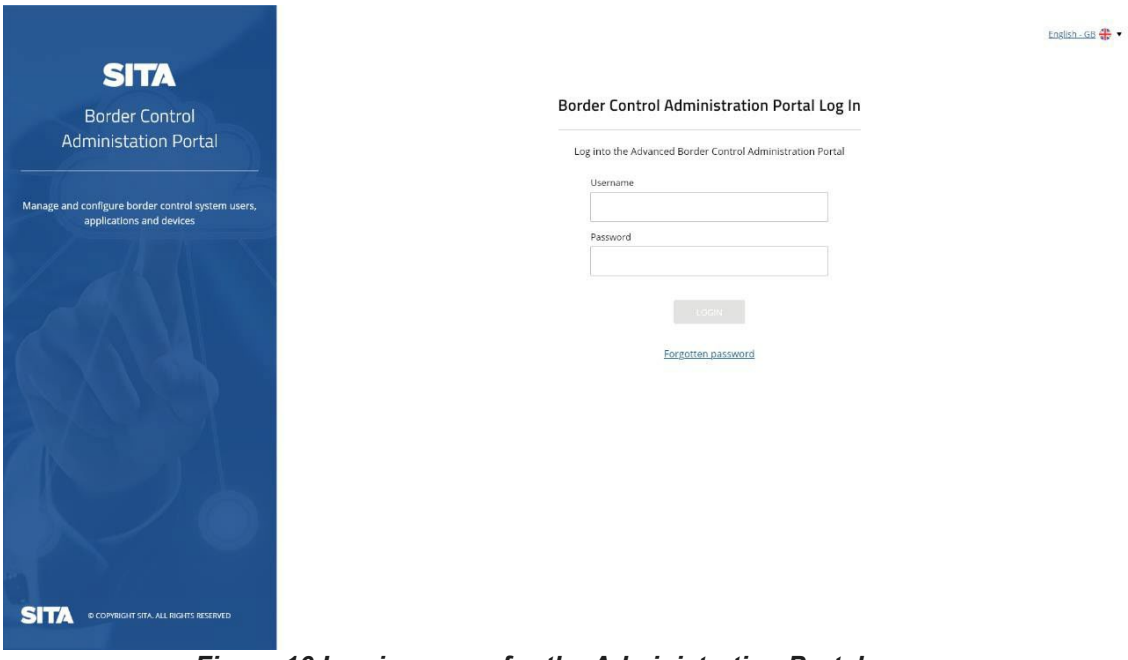


Figure 16 Log in screen for the Administration Portal

Admin portal allows the user based on the role to access dedicated features like reporting.

Central administration of the system is also provided through the "Admin Portal" which provides the following functionality:

Country Codes: Country codes are organized into country groups. We can add and remove country codes from groups,

Location: The code is used by devices for their location configuration. Location codes can define more than the location of the Border crossing, it is defined in a tree structure so the dataset can start at the airport level, then arrival/departure, then specific zones.

System configuration parameters: (thresholds, timeouts, etc.) in all its central and field components, as well as to support specific functional requirements where these require the need to configure specific parameters or basic data.

Other master data will be added into the project based on the initial analysis phase.

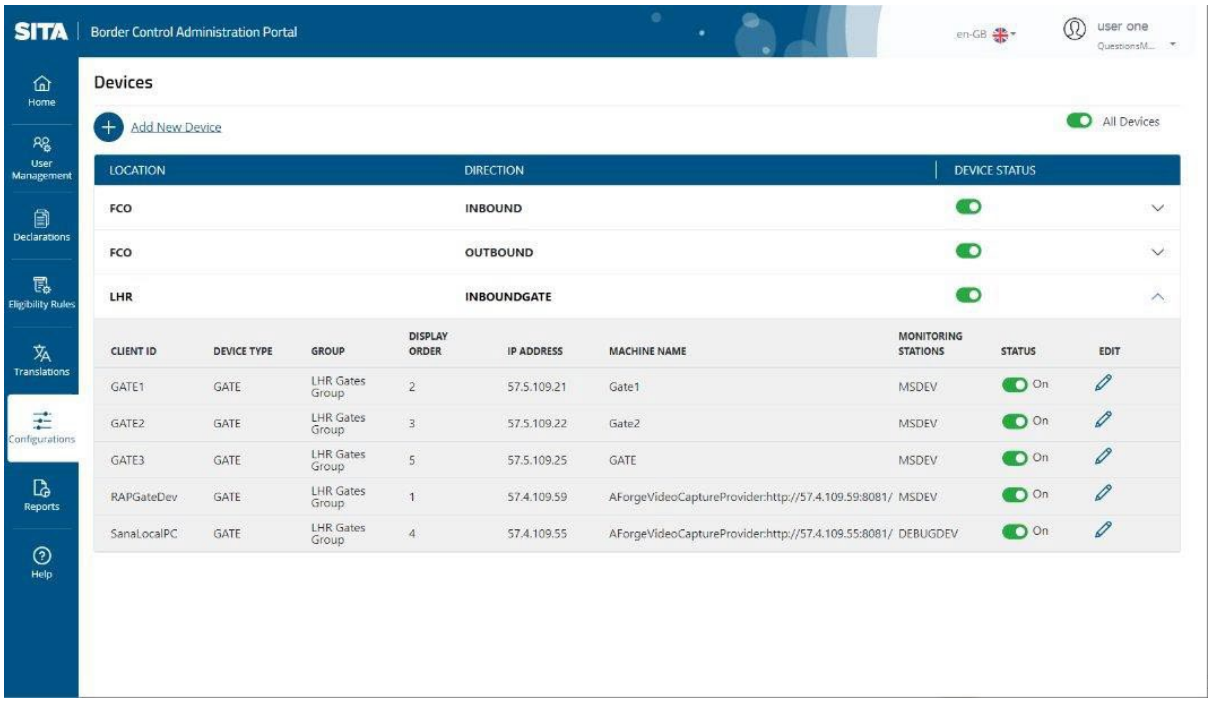


Figure 17 Device Configuration Menu

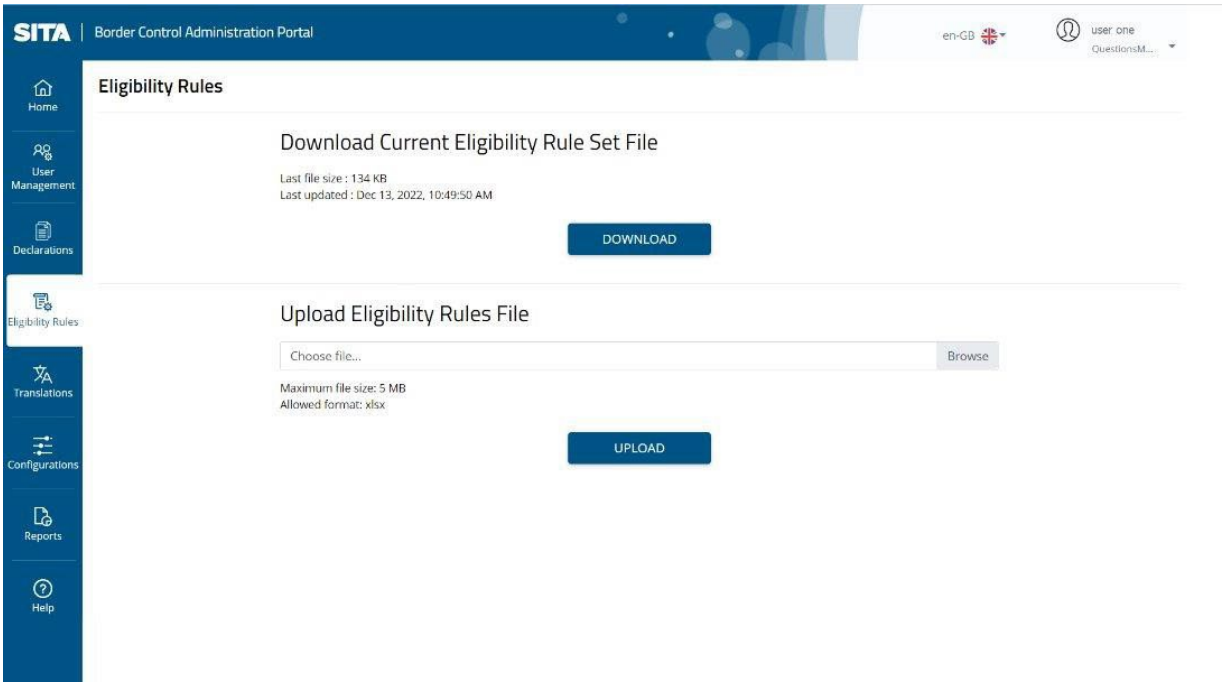


Figure 18 Eligibility Rules Configuration Screen

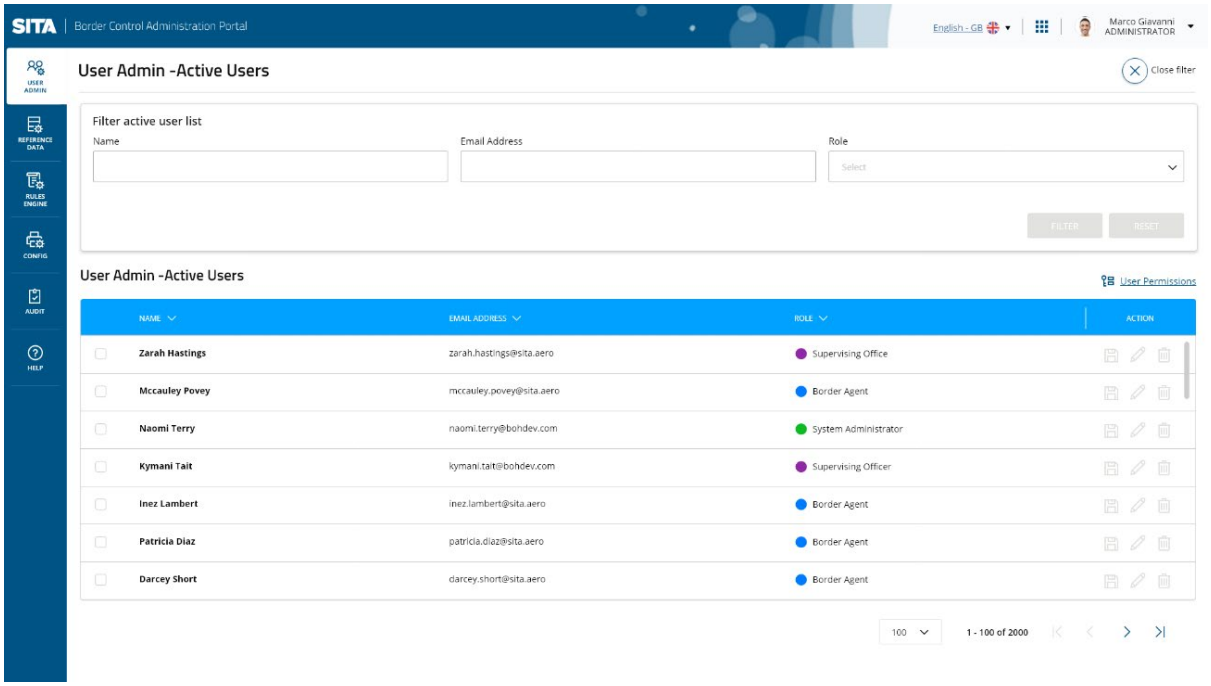


Figure 19 User Management Portal

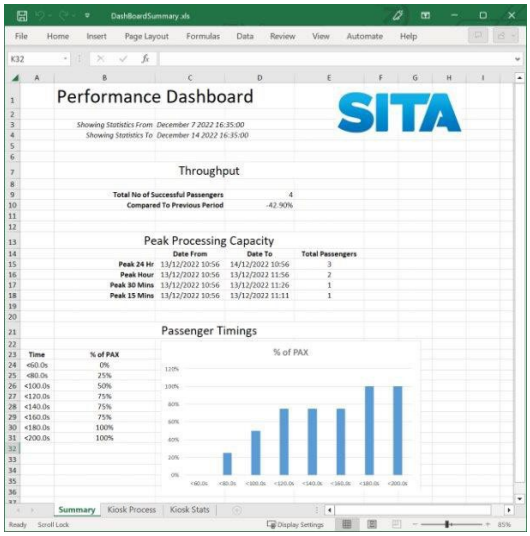
The Admin portal allows the authorized user to manage user profiles. Another option is to get an interface with an external LDAP or Microsoft Active Directory to reuse existing users.

Reports can also be generated using a command line tool by taking filtering parameters and output type (CSV or XLS) as parameters. Reports can be scheduled to be automatically generated in the required format and optionally upload them to specific locations using various options like FTP or SFTP.

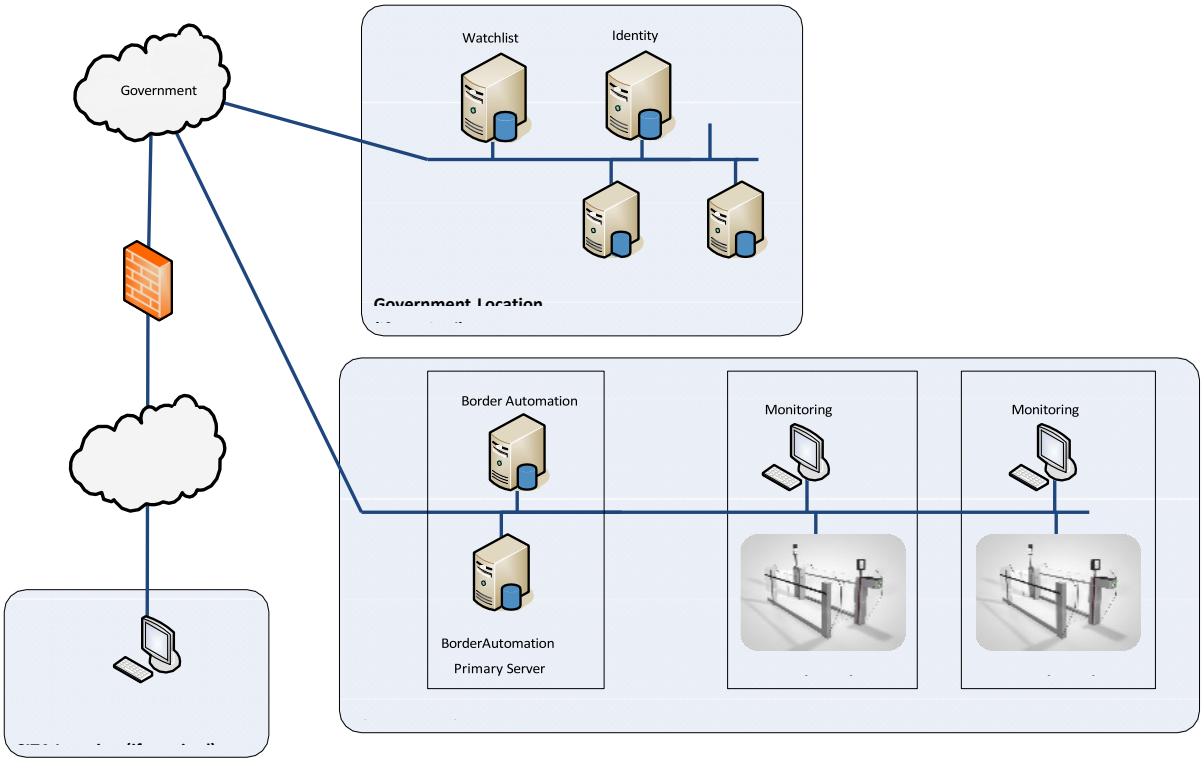
Dashboards, representing key metrics identified during the detailed analysis, will be produced and supported. The dashboard will be part of the administration portal and will be accessible through role- based authentication.

The Admin portal also allows to extract system metrics and reporting. Data can be extracted configuring an automatic task scheduler in various formats (CSV or XLS as preferred formats) for further processing KPI process metrics are aggregated from system logs and include:

- Process time metrics, both end-to-end and step-by-step:
- Quality and control metrics for biometric transactions.
- Number of passengers in the last period (configurable).
- Peak processing capacity over the period (configurable).
- Passenger schedules.
- For the overall activity.
- By steps (passport reading also by nationality.
- Distribution of passengers by nationality, age and gender
- Biometric Performance



4.5 High Level Architecture



4.5.1 ABC Server

The provides central services to the ABC Gates:

- A central point of interface to external systems.
- A central repository of all audits, logging and metric information for the system - all operations and user accesses are properly audited, and all communications between components of the system, as well as sensitive data stored in the database, are encrypted.
- A reporting client provides reports on various aspects of the system, such as statistics on passengers processed and ABC Gates operations (up-time, outages, number of passengers processed by hour, average processing time, etc.).
- User administration functionality - the ABC Gates Server incorporates an operator management and authorisation service to add, manage and remove operators and assign roles system monitoring capability to monitor the status of the individual ABC eGates;

Integration with Government Services

In our assessment of Moldova's border management and immigration processes, this approach remains consistent. The focus of the ABC solution is to ensure secure, reliable, and compliant processing of travellers' travellers under government control, without reliance on airport-side systems. Similar deployments in other countries confirm that national authorities prioritize independent, sovereign control of border automation, which avoids the risks and complexities of integrating with non-governmental airport systems.

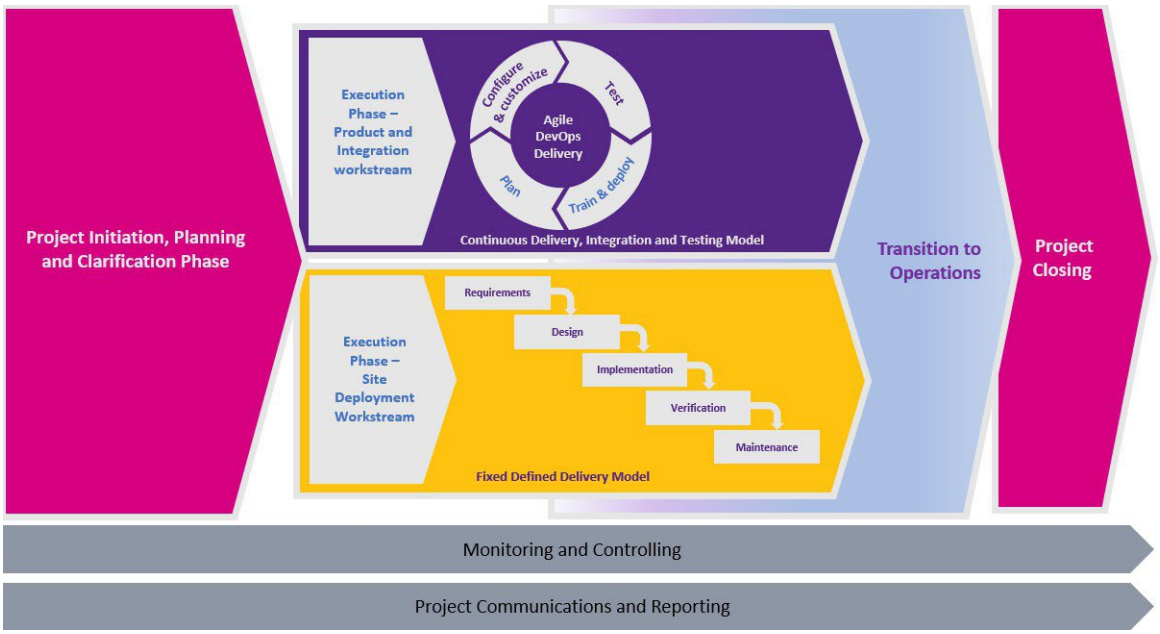
The integration shall be implemented using SOAP-based web services, specifically developed to enable secure and standardized data exchange with IGPF, in full compliance with its protocols and specifications. The detailed design of the integration with IGPF will be finalized during the Design Phase of the project.

5. PROJECT MANAGEMENT, DELIVERY AND INSTALLATION

While every project is different, SITA follows a standard project management methodology framework based on the Project Management Institute's (PMI®) Project Management Body of Knowledge, PMBOK® Guide, and is also successfully used with customers who use the OGC PRINCE2™ methodology. This ensures a rigorous approach for delivering within schedule, with appropriate levels of governance.

The SITA Project Management Competency Program leading to PMI® Project Management Professional (PMP®) certification ensures that our Project Managers are not only competent in the methodology but also equipped with specific personal and professional skills and experience.

SITA has defined this methodology in detail in its Standard Delivery Process, summarised in the diagram below:



The main elements of SITA's Project Management Methodology can be explained as follows:

The Initiation, Planning and Clarification phase is concerned with setting up the project and mobilisation of staff. This is explained in detail in the Delivery Approach section below.

The Execution phase has 2 main workstreams, being Product and Integration, and Site Deployment.

The first workstream is Product and Integration Workstream mainly involved in software delivery, where SITA will use a Fixed Defined Delivery Model augmented by an Agile Methodology, which utilises a Continuous Delivery, Integration and Testing approach

especially for the product development. This approach will ensure a seamless transition to an Agile DevOps approach into the operations phase.

Experience shows that by following this methodology, which will be explained in more detail in the following chapters, we will have excellent results during the Execution Phase for this project.

The second workstream is for hardware installations, rollouts and integration where SITA prefers to use a Waterfall delivery Model. This is because multiple stakeholders and workstreams are involved (such as Infrastructure, civil works and logistics), so it is important to have clearly defined phases and handover points to implement those workstreams in the most efficient way.

The Execution phase is also explained in detail in the Delivery Approach section below.

The Monitoring and Controlling activities are carried out across all project phases. These will include weekly standard project management tools such as schedule management, risk management, issue management. These will be achieved through weekly meetings with customer.

The Project Communications and Reporting activities provide the customer and SITA executive oversight of the project to monitor the project and ensure the swift resolution of any issues.

The Transition to Operations phase is concerned with training and handover activities to ensure the support model is in place. The Production system will therefore run smoothly, and users understand how they can obtain the required support.

Closing a project ensures the project has an endpoint and there is a signoff of the project completion; there will be a transfer of ownership of the project outputs to the customer, their support organisation and the SITA support team. We would run a “lessons learned” activity as part of this phase.

5.1 Delivery Approach

The following sections explain the detailed delivery approach for this project, related to the “Initiation, Planning and Clarification” and “Execution” phases of SITA’s Project Management Methodology. This covers project initiation through to delivery and acceptance of hardware and applications, finishing with deployment and transition into Operations.

Initiation – Hitting the ground running

Project Initiation is concerned with setting up the project, mobilization of staff, confirming the project stakeholders, and creating risks and issues registers, and conducting a project kick-off meeting with the customer.

5.2 Mobilization

SITA will start mobilising the project as soon as the Contract is awarded. This includes assignment of key resources and forming a red team to prepare start of the project and to plan the formal project kick- off.

Any development environments required for the project will be reserved at this stage so that the works can start on time. At this stage, we will also notify our equipment suppliers to give them sufficient time to prepare hardware in advance of the formal order.

Mobilisation in advance of formal project start will enable us to be fully prepared for the formal project kick-off.

5.3 Project Kick Off

SITA will hold a project kick-off meeting with the customer to ensure that all parties have the same vision of the project and are aware of the key success factors. The kick-off meeting is also an opportunity for the key stakeholders of the project from all parties to be introduced and to describe their roles and responsibilities.

SITA will present topics including a high-level view of timeline, key milestones, high-level test strategy and acceptance criteria. Planned Integrations with Government and/or airport systems will be discussed as well.

The discussions during the Kick-off meeting will allow the project schedule and Project Management Plan document to be prepared in conjunction with the customer in a collaborative way.

The following stakeholders are usually present in the meeting:

- Customer representatives – usually from Operations- and IT-Department, Terminal planning
- Immigration Department/Border Police
- SITA Senior Project Management
- SITA Business Development
- SITA Solution Design/Business Analyst
- SITA Support Management

More immediate actions such as arrangements for security clearance and to survey the key sites and applying for accesses and health & safety training for SITA personnel will also be discussed and started immediately. This will allow SITA to prepare any necessary paperwork and applications as early as possible.

5.4 Site Survey Plans

A detailed site survey of Chisinau International Airport is important at the beginning of the project, to make an assessment of the environment and to identify any potential issues such as lighting conditions, storage on site, proximity to power and network points, and logistical consideration of transporting the equipment to its final location.

This will also allow us to identify precise locations of the ABC eGates, and any capital works required including Health and Safety requirements.

General rules are that uniform lighting of the passenger face is required to get optimal performance from the biometric algorithm, and no windows or bright light should be in the direct vision of the camera.

5.5 Detailed Project Schedule

This activity confirms the schedule in conjunction with the customer and involves elaboration and establishment of a baseline project schedule. This requires input from customer and its stakeholders.

This draft plan will be presented in a workshop setting and any feedback will be incorporated into the plan.

The baseline project schedule will identify those activities on the critical path, or near to the critical path, so that they can be monitored closely to avoid any schedule slippage. Typical critical path activities are likely to include hardware ordering, delivery logistics including customs clearance and installation.

5.6 Project Management Plan

The SITA Project Manager will finalise a Project Management Plan (PMP) document which covers in detail important aspects of the project delivery, such as:

- Implementation approach, deliverables, milestones and dependencies
- Communication Plan
- Roles and Responsibilities
- Quality Management Plan
- Risk Management
- Issue Management
- Change Management
- Project Governance

The PMP will ensure that there is a common understanding of the way the project will be managed.

5.7 Site Deployment

Deploying the ABC Gates into Chisinau International Airport can be complex from a logistical perspective. Clear planning and scheduling with all stakeholders are key, so that any capital works and installation is aligned with the customer airport own infrastructure master plan.

SITA has a substantial presence in customer airports, where our Operations and Delivery Managers have experience working with airport authorities and understand the stakeholders and processes required for this deployment. These embedded SITA resources will work closely with the Deployment Team led by an Infrastructure Project Manager to produce a Deployment Plan and ensure a well- planned a

d executed implementation.

Further, the Deployment Team will be utilising detailed Delivery Guides which are the products of SITA’s extensive experience in this activity and augmented with lessons learned from other projects.

5.7.1 Hardware and Applications Installation

Hardware installation covers the server equipment that would be installed at the Government data centre, and the site installations and pre-Production facilities for the ABC Gates. SITA's experience working in high security data centres and locations has resulted in a strong understanding of the constraints of working in such locations.

Applications are then installed on the staging servers in anticipation of acceptance testing. SITA can physically carry out this installation if remote access to the data centre is restricted by Data Centre security policies.

SITA also recognises that airports are busy environments with complex operational activities being carried out around the clock, and that disruption to such activities can result in high impact to airport workers and passengers.

SITA will prepare installation plans at each site with appropriate stakeholders to minimise such disruption and fit in with the airport master capital works plan.

The SITA Infrastructure PM will also be present on site overseeing the delivery and working with the stakeholders to carry out the installations.

5.8 Training Plan

Our Training Manager, in consultation with your appointed Training Managers, will provide training plan during the project.

The plan shall include the following:

- Definition of user/engineer roles
- Course descriptions, target audience, format, duration, objectives and content
- Mapping of user/engineer roles to courses
- Schedule of training (including date, duration, venue of the training)
- Logistics requirements.

Work on the training plan will commence at the start of the implementation phase of the project and will be constantly reviewed as delivery progresses.

The training plan will also identify any ongoing training that will be required as the system is upgraded during its lifetime.

5.9 Resource Requirements

Role	Duration/Task
Project Manager	Manage project deliverables and manage risks and potential issues.

Role	Duration/Task
Implementation Engineer	Deployment of servers and software. KT to some Border Police, and Operational Staff. Providing details for interlock with development team on bugs and issues.
Business Analyst	Support for changes in workflow or requirements if necessary and providing relevant documentation for customer sign-off. Acceptance Criteria and UAT
Solution Designer	Technical workshop support, if necessary, e.g. further integration explanation. Support for changes in the solution if necessary. Solution Documentation and requirements matrix.
Training Support	Support/ Train the Trainer fact to Face
Transition Management	Transition documentation and drive necessary tasks for transition, aligning delivery to fulfil the agreed operational model. Covering upgrades too.
CSM	Support in Airport operations readiness and local supplier operations readiness, clear SOPs and Operational Guides.

6. SUPPORT MODEL

SITA understands the nature of mission-critical border management processes. We offer a full range of support services designed to achieve up to ultra-high availability, 24 hours a day, 7 days a week, covering the lifecycle of our products and services. Support can be delivered on-site, or via remote management from the Service Desk. When and where required, SITA will utilize local partners to ensure the same level of service is delivered.

The primary goals of SITA's Incident Management processes are to maximize "normal service operation" and minimize maintenance costs. The Service Desk enables the opening, fulfilling and closing of customer requests. It focuses on resolving the call, utilizing First Call Resolution (FCR) techniques before dispatching to other support teams. The Service Desk and support teams use remote monitoring, remote intervention and remote takeover tools to provide immediate fixes and to minimize on-site interventions.

SITA's service and support processes are derived from extensive experience in supporting mission- critical operations for its customers and are documented using ITIL terminology and conventions. (ITIL is generally recognized as the best practice approach for IT Service Management and is adopted by thousands of organizations worldwide). Support is designed to provide long-term assistance in maximizing the effectiveness of any deployed solution. The goal is to preserve the highest degree of customer satisfaction by maintaining problem-free system operation.

6.1 Support Model Overview

It is proposed that SITA will support and operate the proposed modules of the ABC Gates with the assistance of our local partner the customer's resolver groups, when necessary, to provide second and third level support for the delivered system for the life of the contract. The Support can be provided by SITA directly or using an approved local partner.

The operating model will be as follows:

- Incidents will be reported by administrators and users to the Government Service Desk and dispatched to the SITA Service Desk to initiate the relevant support procedure.
- SITA fault resolution groups will then work over a remote network connection and/or with the assistance of on-site support staff to rectify the incident where necessary.
- SITA will provide support for the solution hardware (including regular backups) installed in the Data Centre. The support model described in the subsections has been designed in adherence of ITIL Best Practice, and comprise of:
    - SITA Central Service Desk providing Level 1 support on 24 x 7 x 365 basis
    - SITA Local Team providing Field Service Support 8x5, Normal Business Hours
    - SITA Central Level 2 support on 24 x 7 x 365 basis
    - SITA Application Support Level 3, operating 8x5x5, Normal Business Hours

- Customer Service Management for the service and will attend agreed Service Review Meetings remotely.

6.2 Service Levels

6.2.1 Service Availability

Service Availability Achieved is measured against the Service Availability Target and is calculated as a percentage of the maximum service availability period. The table below contains a calculation **(provided as an illustration only)** of Service Availability Achieved during a measurement period of three (3) calendar months.

A quarter based on 90 calendar days = 129,600 minutes (for a Service cover period of 24 hours x 7 days a week)
Scheduled Downtime and/or unscheduled permitted downtime = 240 minutes
Time related to Force Majeure Events and/or exclusions = 240 minutes
Maximum service availability period = 129,120 minutes
Unplanned Outages = 600 minutes
Service Availability Achieved for relevant measurement period = ((129,120 – 600) / 129,120) * 100 = 99.53%
If Service Availability Target = **99.0%**, the target is exceeded.

6.2.2 Service levels for production Service Availability are as set out in the following table and are limited to SITA provided Services, infrastructure, hardware and Software:

Service	Service Cover Period	Service Availability Target
SITA ABC Gates	24 x 7 x 365	99.000%

Restoration of Service Time

6.2.3 SITA reserves the right to modify the applicable Service level targets for Site Availability, where a resilience design of the Service is modified by the Customer at a Customer Site.

6.2.4 When the Customer reports an Incident to the SITA Service Desk, the SITA Service Desk will assign to it one of the priority levels defined below.

6.2.5 The call will be assigned a priority code, agreed between the Customer and SITA upon logging the call. The list of priority levels and associated criteria and definitions shall be defined as specified below:

Priority Level	Description & Criteria	Priority Definitions
1	**Critical Impact on Business** Total system failure and interruption of business-critical applications affecting the entire system. Alternative or bypass is unavailable.	**A fault that seriously affects the normal daily operation and needs to be fixed at the earliest opportunity.** **Impact/Urgency: High/High** **For ABC Gates: 100% of devices would be unavailable.**
2	**Serious Impact on Business** Major Business Impact: Complete or partial service interruption of business-critical applications. Acceptable bypass is available.	**A fault seriously affecting the normal daily operation but not yet causing critical impact to the daily operation.** **Impact/Urgency: High/Medium or Medium/High** **For ABC Gates: 75% - <100% of devices would be unavailable.**
3	**Impact on Business Efficiency** Minor Business Impact: Partial service interruption of business-critical applications. Operational impact is minimal with no immediate impact on service operations. Alternative bypass is available.	**An incident which does not seriously affect the day-to-day operation. A workaround exists and/or the problem will be addressed in the next release of the Service Application.** **Impact/Urgency: High/Low or Medium/Medium or Low/High** **For ABC Gates: 50% - <75% of devices would be unavailable.**
4	**Inconvenience to the Business** Minimal Business Impact: Component, procedure, or personal application not critical to a customer is unusable. Alternative is available; deferred maintenance is acceptable (problems reported to suppliers). Impact to service operations minimal; possible minor inconvenience.	**Medium - partial service interruption with no impact on customer's operations.** **Impact/Urgency: Medium/Low or Low/Medium** **For ABC Gates: 0% - <50% of devices would be unavailable.**
5	**No Business Impact** **No Business Impact: Non-service affecting faults or request to change. Alternative or bypass is not applicable.**	**Low – Non-operational request (for information, request for change - rarely used)** **For ABC Gates: Experiencing intermittent issue(s).**

Automated Fault Detection

6.2.6 SITA will operate a range of automated tools to establish the health of hardware and Software applications. In the event of a suspected problem, the SITA service desk is automatically informed and will take the appropriate

action, logging a call and passing it to the relevant Level 2 Resolver Group which will then investigate for resolution.

6.3 Incident Response and Restore Time

6.3.1 The Time to Restore is calculated as the elapsed time.

6.3.2 SITA will put processes in place designed to meet the target mean time to restore timescales specified in the table below:

Priority Code	Response Time	Update(s) to Customer(s)	MTTR
1	30 min	1hr	4 Hours
2	30 min	1hr	8 Hours
3	30 min	6hrs	1 Business Day
4	30 min	12hrs	2 Business Days
5	30 min	1 Day	5 Business Days

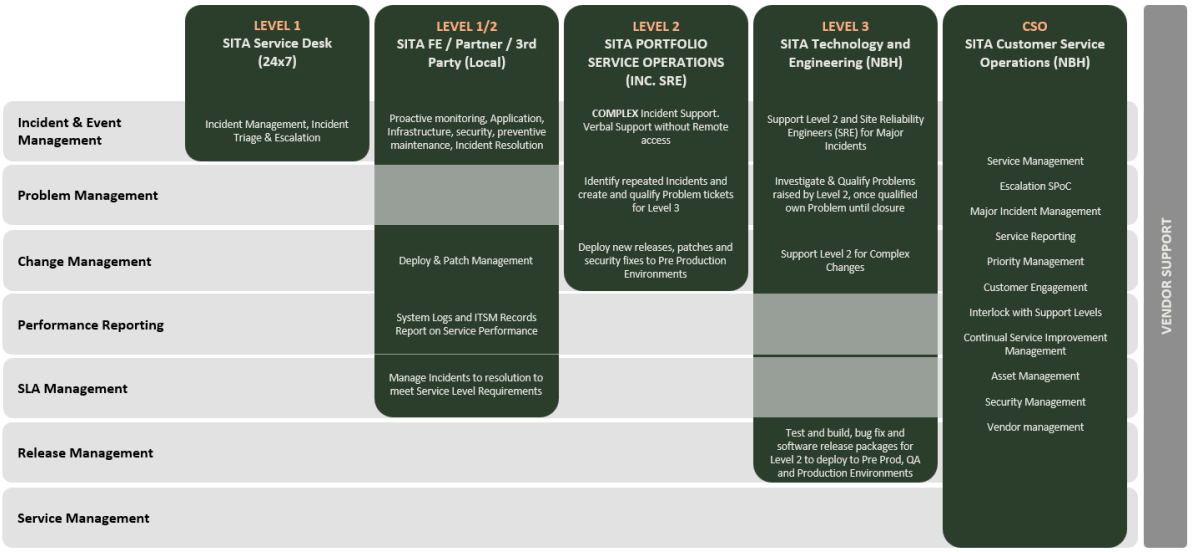
6.4 Service Level Exclusions

6.4.1 The Service level / availability / performance is not applicable in the following circumstances:

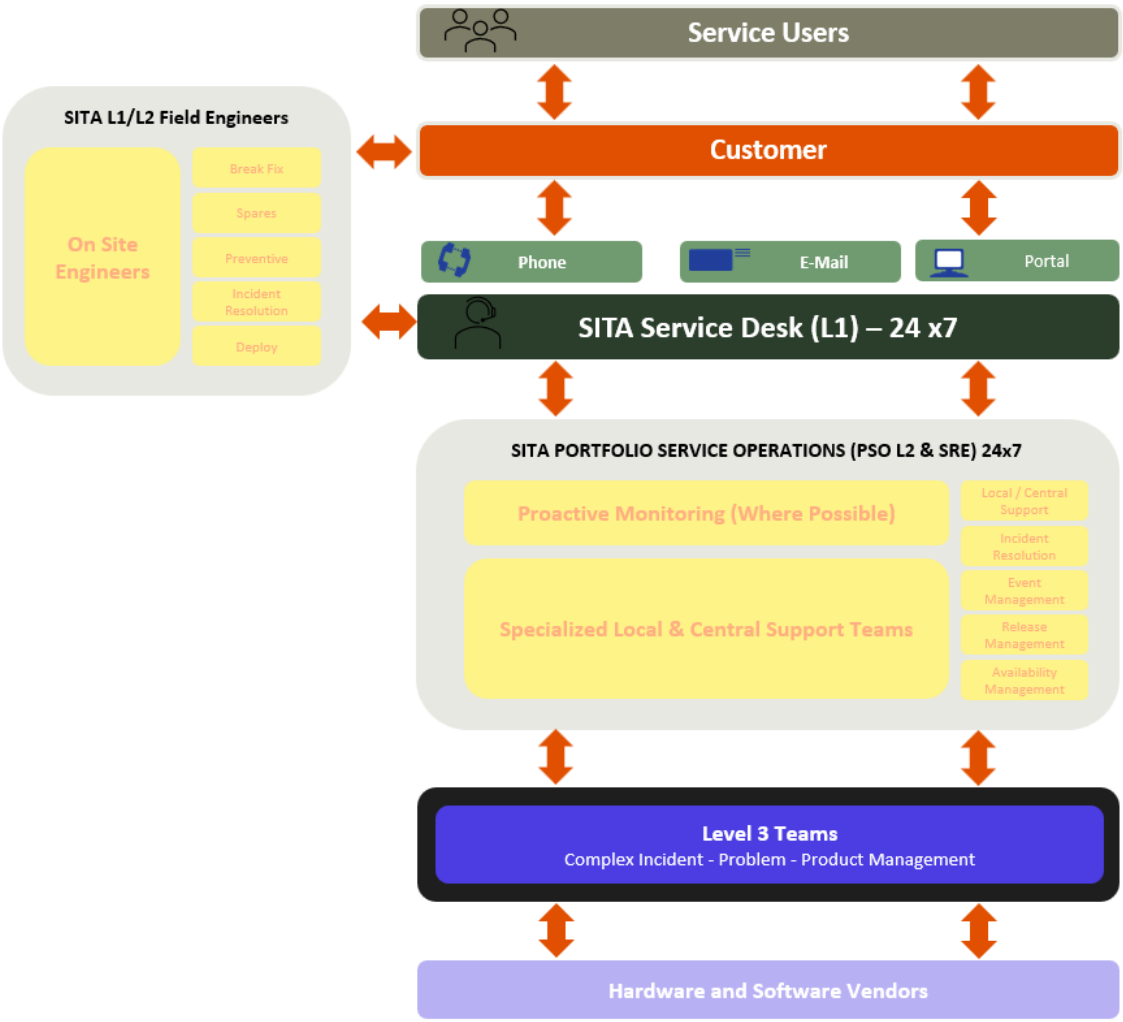
- in case of Scheduled Downtime.
- in case of emergency maintenance notified to Customer as soon as reasonably practicable.
- in case of incomplete or missing data.
- in the absence of an Incident record issued by the SITA Service Desk.
- during Defer Time.
- Outside the Service cover period.
- If root cause is the same (repeated).
- Customer application outages SITA services may rely on for interaction and data validation purposes.
- Degradation is not a service level impacting state.
- Equipment, services and third-party applications hosted and supported outside of SITA’s control.
- Downtime caused by equipment, services and/or third-party applications, connections and Software outside of SITA’s control.

6.5 Maintenance and Support Elements

6.5.1 In relation to this Service, SITA will provide Customer maintenance and support services, comprising the following elements, excluding any services, infrastructure or server hardware and software provided by Customer. The diagrams below show the various levels of support, areas of responsibility, a second diagram showing support flows, followed by a more detailed description of the service provided.



SITA Service Operations Responsibility Matrix



SITA Service Operations Flow

6.5.2 Level 1 Support- Service support through the SITA Service Desk, which provides:

- Incident management and Incident resolution.
- Escalation management.
- Problem management.
- Change management.
- Event management (Proactive monitoring when remote access is in place).
- Preventive maintenance.

6.5.3 Level 1/2 Field Services – Support through local field engineer team which will be provided through a 3rd party in-country provider.

6.5.4 Level 2 Support - Service support through the SITA Portfolio Service Operations Team.

6.5.5 Level 3 Support - Service support through the SITA Technology and Engineering Team.

6.6 Level 1 Support - SITA Service Desk

6.6.1 The SITA Service Desk will:

- be the owner of Incidents responsible for ensuring that all Incidents are recorded and managed to successful resolution.
- provide resources to deal with Customer user enquiries and to handle Customer's Service requests.
- monitor the timely handling of the Incident by each assigned Resolver Group initiating escalation actions as required; and
- provide services in English.

Incident Management

6.6.2 Incident management is triggered in several ways:

- by Customer reporting the Incident to the SITA Service Desk by mail or phone call.
- by Customer reporting the Incident through SITA Service Management Portal; or
- by a defined actionable event being observed as part of remote management services (limited to when proactive monitoring is contracted).

6.6.3 The following applies to Incidents raised through the SITA Service Management Portal:

- The status and progress of Incidents are communicated to Customer through the SITA Service Management Portal and email.
- Customer can communicate with standard service desk by email/phone and through the SITA Service Management Portal; and
- Customer can escalate.

6.6.4 The SITA Service Desk will perform the following actions for reported Incidents:

- log and categorize reported Incidents.
- track the Incident through to resolution.
- provide status updates to Customer.
- engage appropriate Incident resolution resources.
- escalate to appropriate Resolver Groups and levels of support.
- identify known errors and repetitive Incidents, providing a workaround where applicable.
- verify closure with Customer and, where applicable, obtain Customer concurrence for Incident closure.
- respond to Customer User queries regarding Incidents.
- initiate Customer communications during critical situations.
- initiate escalation procedures for critical situations; and
- close the Incident record and document the Incident resolution.

Incident Resolution

6.6.5 SITA shall perform the following activities when required to resolve Incidents or to resolve or avoid Problems:

- investigate and diagnose the cause of repeated Incidents and Problems.
- take appropriate actions to resolve Incidents and Problems.
- apply emergency software patches and updates when required.
- update configuration information when required; and
- ensure that other related activities are reported and recorded by the SITA Service Desk.

6.6.6 Upon detecting an actionable event, or notification of an Incident to the SITA Service Desk, remote management tools will be used to investigate and resolve the Incident.

6.6.7 When appropriate, SITA may use remote management tools to address Customer's service needs.

SITA will:

- define a security policy and procedures for remote management access.
- obtain Customer's permission to perform a remote workstation takeover, if required; and

- establish a schedule for remote management adjustments to be made and advise Customer, if requested.

Escalation Management

6.6.8 Should an Incident not be resolved within the applicable Service level targets, the SITA Service Desk shall provide status updates to Customer in accordance with agreed procedures.

6.6.9 The SITA Service Desk may trigger escalation procedures when an Incident resolution time is in danger of exceeding the threshold defined in the Service Levels Schedule.

6.6.10 The objectives of the escalation procedures are to ensure that:

- an Incident is rectified as quickly as possible.
- all measures are taken to minimize any disruption to Customer's operations.
- if an Incident cannot be resolved within pre-determined periods, affected Customer users are notified of the Incident and the progress of its resolution.
- appropriate and progressively, more senior SITA staff are made aware of the Incident and the actions being taken for resolution; and
- appropriate resources are deployed as necessary to assist the resolution effort.

Problem Management

6.6.11 SITA will provide Problem management to identify, remove the cause and minimize the impact of repeated Incidents and Problems on Customer's business.

6.6.12 The Problem management team will work to identify the root cause of the Problem, initiate corrective actions, and resolve the Problem.

Change Management

6.6.13 Customer can submit Change Requests through SITA Service Management Portal or email to SITA Service Desk.

6.6.14 Customer can request simple changes using the standard change catalogue. These changes are managed by Standard Service Desk who can interact with Customer using the SITA Service Management Portal.

6.6.15 Customer can also submit Change Requests, through SITA Service Management Portal, outside the change catalogue using free text fields. These changes are redirected to the Customer's account manager.

6.6.16 Some Change Requests are chargeable on a per completed transaction basis, in addition to Service(s) charges.

6.6.17 SITA will advise Customer of Changes proposed by SITA with sufficient details on change plan and foreseen impact to Customer services.

Event Management (Proactive monitoring)

6.6.18 The SITA Service Desk will also act in operational synergy with the SITA Field Services Team where Event Management is not possible to manage remotely. The SITA (3rd Party) Team operates the event management process and detects any deviations from the normal state of a Service. Events are typically notified by an alert which is then made known to staff, when monitoring the tool directly, by a screen alert and/or audible alert as well as email notifications. Events are provided by monitoring and control systems which are based around two types of tools:

- active monitoring tools to determine the status and availability of a configuration item (for example warning that disk capacity is nearing a pre-set limit).
- passive monitoring tools that alert when an operational situation has occurred (for example, a fire alarm where possible).

6.6.19 In general, event management will be used for the following Service management aspects where possible:

- hardware status, performance and utilization.
- environmental conditions.
- Software utilization and monitoring; and
- security intrusion detection.

6.7 SITA Field Services

The SITA Field Services will maintain the equipment, within SITA's are of responsibility, installed at site in working order as described below, these activities would be performed in the main by SITA's subcontractor for maintenance and support of SITA's solution in country, provider of SITA certified service centre with certified engineers:

- Corrective maintenance
    - Perform break-fix activities on the hardware units. This can result either in repairing the faulty unit or replacing it with a spare where availability permits,
    - Support SITA remote teams with troubleshooting and service restoration activities,
- Preventive Maintenance
    - Execute preventive maintenance in accordance with SITA or manufacturers' instructions,
    - Periodically inspect the equipment to ensure their working order (e.g., cabling, power),
    - Detail of Preventive maintenance activities shown in table below

Checklist for Preventive/Corrective Maintenance	
Daily Maintenance	Review previous day's Operations Shift daily status report.
	Review monitoring tool for any alarms (Notifications, Warnings etc.) including performance checks.
	Review operational emails for system alerts and notifications.
	Review ITSM Tool for Incident Creation and Status and update where applicable.
	Validate any alerts raised, relevant emails raised.
	Work on any open incidents, problems, and changes.
	Review previous day's Operations Shift daily status report.
Per Device	Visual inspection: Check for any obvious damage or wear and tear on the gate and surrounding areas. Look for loose or damaged components, obstructions, or unusual noises.
	Sensor check: Verify that all sensors are clean and functioning correctly. This may involve wiping down sensors and ensuring they are not blocked.
	Clearance check: Ensure there is sufficient clearance around the gate for proper operation and to prevent accidental contact.
	General cleaning: Wipe down the gate and surrounding areas to remove dirt, dust, or debris.

Checklist for Preventive/Corrective Maintenance	
	Check and clean physical device(s) surface with Isopropyl Alcohol (min 70%) on a cloth where surfaces are in contact with customer/user.
	As and when required: o Remove foreign objects (gum, paper, coins etc) from physical devices such as reader, camera etc. o Clean outer surfaces with non-chemical liquids, use a damp cloth, do not apply anything liquid direct to surface or equipment.
Daily Maintenance Server Room Where Applicable	Environmental Monitoring Activities (Room Temperature, Humidity, Water Leakage).
	Check server access (Virus Protection, Security Patch Management, System Auditing, Access User Policy Enforcement).
	Server health checks, disk space, memory, CPU, data processing state via monitoring toolsets.
	Database checks (such as table space, any database errors).
	Check backup status.
Document	At end of each activity document in the shift handover document ready for the team to email full daily status report for the morning shift.
Weekly Maintenance	Detailed inspection: Perform a more thorough inspection of all components, including the motor, drive mechanism, and control system.
	Lubrication: Apply appropriate lubricants to moving parts as per manufacturer recommendations.
	Sensor calibration: Calibrate sensors to ensure accurate and reliable operation.
	Software updates: Check for and install any available software updates for the gate's control system.
	Operational testing: Test the gate's functionality under different conditions to ensure it is working as expected.
Document	Record details of checks in Shift Handover document.
Monthly Maintenance	Component replacement: Replace any worn or damaged components, such as belts, rollers, or sensors, as per the maintenance schedule.
	System diagnostics: Run diagnostic tests on the control system to identify any potential issues.
	Emergency stop function test: Test the emergency stop function to ensure it is working correctly.

Checklist for Preventive/Corrective Maintenance	
	Have Power supply checked: Verify the power supply is functioning correctly and that all connections are secure.
	Incident review, look for repeated issues and generate associated Problem Ticket in ITSM Tool
	Generate any statistics for monthly reporting (SLA Report)
	Knowledge sharing within the team
	Server/Storage/Network Equipment Firmware/Drive Code Patch Review/Performance Review
	Monthly Operations Review Meeting (Review Incidents, Problems, CRs)
	Validate that monitoring agents are functioning correctly
	Check ABC PC such as fans to make sure clear of dust and dirt, vacuum where appropriate
Document	Record details of checks in Shift Handover document.
Quarterly Maintenance	WAN checks (configuration validation for high availability).
	Capacity review.
	Backup test restores.
	Asset Management Review
	Documentation review
	Review security policies
Document	Record details of checks in Shift Handover document.
Annual Maintenance	Backup media retention/distribution.
	Backup media replacements if applicable.
	Contract review.
	License & Certificate review.
	Service Benchmarking.
	Service Improvement Review
	Production to Standby/DR failover test (Including Business Continuity)
	WAN checks (test resilience)

Checklist for Preventive/Corrective Maintenance	
	Network and Security Policy Review
	Hardware Review
Document	Record details of checks in Shift Handover document.

Preventive Maintenance Check List

- Warranty Management
    - Manage the shipping of parts requiring repair or replacement to the vendors.
- Spare management
    - Monitor spares movements and manage spares inventory and replenish spares stock as required to maintain an adequate level of spares.
- Other activities
    - Perform IMACD (installation, move, addition, change or decommissioning of equipment) activities requested by the customer through Change Control.
    - Produce reports or raw data to support SITA Customer Success Manager with reporting and problem management activities,
    - Record and update the detail and status of the support provided for incidents, changes, and service requests on SITA ticketing tool, SITA Service Gateway.
    - Ensure that SITA CMDB is kept updated following the execution of activities, for example hardware replacement.

The Field Engineering team will be supported remotely by SITA support teams to which complex technical issues can be escalated as required.

6.8 Level 2 Support - The SITA Portfolio Service Operations (PSO)

6.8.1 Monitoring and fault management will be provided by SITA Portfolio Service Operations Team (PSO), including all remote activities (when remote access is available) such as trouble shooting, diagnostic, restoration and other remedial activities required in order to restore a Service application to a full operational mode, excluding any infrastructure, hardware or software provided by Customer. Level 2 Support will provide the following services, where remote access is not available SITA Field Engineering services are utilised with backup support from Level 2:

- platform software updates; and
- launch application updates.
- perform Incident resolution or identify Problems where root cause is unknown.

- notify the SITA Service Desk when onsite technicians need to be dispatched for hardware break/fix.
- escalate to L3 support team (the Problem management team).
- perform workarounds identified by the Problem management team for Incident resolution.
- identify changes to infrastructure\software required for Incident resolution.
- notify SITA's Application Management team(s) of any hardware change that may impact the applications running on that hardware.
- receive global work order notification when new release is available.
- perform System change to deploy new software release; and
- notify SITA Service Desk upon completion of any Change or resolution of any Incident.
- platform software updates; and
- launch application updates.

6.9 Level 3 Support – Site Reliability Engineers and Technology and Engineering team (T&E)

6.9.1 SITA's Portfolio Service Operations (PSO) Site Reliability Engineers (SRE) owns the following responsibilities:

- receives requests for complex Incident (including Major Incidents) and Problem management support via Level 2 Support teams.
- performs root cause analysis to identify bugs or requirements for code change.
- engages SITA's development team to fix bugs.
- test Software fixes prior to deployment.
- apply code changes in next Service application release.
- notifies SITA's operational release management team of upcoming release availability.
- performs recommendation and action planning to update obsolete resources and migration to new versions of software and/or platforms; and
- performs small developments: monitoring shell scripts, scheduled tasks, delete logs.

6.9.2 Level 3 support is complemented by SITA's development, certification group that owns the following responsibilities:

- develop required code change and bug fixes.
- perform certification and testing of new releases.
- make releases available to SITA's airport operations team for global release following beta certification.

- notify SITA's airport operations of availability of a new release; and
- develop functional and technical documentation associated with new developments, user manuals for the scheduled tasks and shell scripts. SITA's development support coverage hours are based on SITA's normal business hours for Level 3 support (Monday - Friday, 9.00 am - 17.00 pm [*GMT+0*]).

6.10 Customer Service Operations Manager (CSO)

6.10.1 SITA will assign a Customer Success Manager (CSM) to manage the operational relationship between Customer and SITA and be the voice within SITA. The CSM will:

- Coordinate release and change management activities to ensure no disruption to the service.
- Manage Availability and Capacity management processes.
- Be the first escalation point for customers, with access to all required SITA management levels.
- Provide monthly reports and present them during regular service review meetings as per the frequency agreed with customer.
- Ensure that SITA is achieving its contracted obligations, addressing any service deviations, and managing any service improvements to completion.
- Perform the role of the Problem Manager, analysing trends, and coordinating any problem management activities, including knowledge management.
- Own and delivery the actions identified and recorded in the Continuous Service Improvement Plan.

6.11 Customer Responsibilities

6.11.1 Customer's responsibilities include (at Customer's cost):

- support, updates, security patching and fault resolution for all customer provided services, infrastructure, hardware and software utilized for the delivery and operation of SITA services.
- provide additional training to Customer users should SITA feel that lack of training is contributing to levels of Incidents.
- ensure basic support for the equipment or the authorized Customer equipment is conducted by the Customer users, including restarting servers/workstations when it is not possible to do remotely due to loss of control.
- report Incidents to SITA as soon as they occur with full details, where known.
- submit Change Requests to SITA, with a clear definition of requirements.
- agree with SITA a timetable for any planned Changes that require work to be done by SITA.

- supply SITA with Customer user contact details.
- ensure that the installation of other hardware at the site will not cause interference to the equipment or authorized Customer equipment, which SITA has agreed to support.
- provide stable secure remote connection for remote Resolver Groups where possible; and
- when required, secure/obtain required access permission for field service Resolver Group.

6.12 Service Levels Report

- SITA shall use reasonable endeavours to deliver within thirty (30) days from the end of each measurement period to Customer a report, which indicates the shortfalls in the Service levels during that measurement period and any SCUs accrued, where applicable, to Customer (Service levels report).
- The parties agree that all information contained in Service level reports is Confidential Information of SITA.

6.13 Spares Management

- The system is provided with an appropriate stock of spare parts which should be kept on-site to facilitate fast repair of components that are more likely to fail over time. SITA recommends that this spare parts kit is kept stocked while the system is operational.

6.14 Preventative Maintenance

- Where required and included in the scope of services, the on-site field services team will provide routine preventative maintenance to mitigate the risk of system failure.

6.15 Scheduled Outages

- It may be necessary to schedule occasional downtime for software updates, network enhancements or other scheduled maintenance as SITA shall decide. Wherever possible, SITA shall consult with Customer to ensure such events are planned to cause minimum disruption.
- In the event of necessary maintenance by SITA that is likely to affect the Service, SITA will provide seven (7) days' notice where possible to Customer prior to any planned maintenance, with the reason, date, time and estimated duration. For urgent, emergency and business critical changes SITA will endeavour to provide as much notice as possible.

- If the Service must be suspended for reasons beyond the control of SITA, then SITA will endeavour to provide the earliest possible notice of such action, an estimated duration and keep Customer updated at two (2) hourly intervals.

6.16 System Freezes

- From time to time, SITA may, for operational reasons, impose a system freeze. SITA will provide seven (7) days' notice of scheduled freezes however there may be emergency situations that mean notice will be less than this. During the freeze period changes to the system shall be restricted or prohibited according to the details as supplied by SITA and during system freeze periods the SITA will not be able to add, amend or remove Services.

7. LEGAL NOTICES

7.1 Contractual Terms

- The delivery of the products and services described in this proposal will be subject to a contract to be negotiated between the parties.
- This proposal is submitted on the basis that the agreement reached between us will be subject to the standard-issue Draft Contract issued with the RFP, subject to any amendments that are mutually agreed. SITA has submitted a list of 'Comments and Observations' on that Draft Contract, which include suggested changes to the Draft Contract presented.
- The information provided in this proposal is confidential to SITA. It may not be shared outside your organization without SITA's express written consent. SITA hereby gives you consent to use and make a reasonable number of copies of the proposal for the evaluation of the proposal only.
- In providing this proposal, SITA has relied upon information provided by you and your partners and affiliates. Accordingly, any change to the information provided or any omissions from it may result in changes to the proposal or to the pricing submitted as part of it.
- All products, services, company names, trademarks, logos, devices, symbols or other similar items (whether registered or unregistered) that may be contained within or referred to in this proposal are acknowledged as belonging to or licensed to the originator.
- The prices listed in this proposal do not include custom duties, value-added taxes, turnover tax, sales tax, and any other tax or duty levied by authorities in relation to the products or services. All such taxes (except any income tax payable by SITA) and/or duties will be charged separately as per negotiated contract.

7.2 Validity Statement

- This proposal and any prices herein are valid for the period specified in the RFP.
- SITA reserves the right to modify the prices or withdraw the proposal after expiry of the validity period.

7.3 Pricing Assumptions

- Prices quoted in the RFP response are in Euros
- Payment will be made in Euros
- Payment terms per the RFP are 20 days upon receipt of invoice
- SITA's price assumes support and maintenance of the solution will be provided for 36 months with spare parts included for a further 24 months.
- SITA's price is based on a CAPEX/OPEX structure, whereby there will be a price related to the delivery and Hardware of the contract and the support and

maintenance will be invoiced monthly over the 36-month operational period. Example of price breakdown in table

Milestone	Price excl. VAT EUR	Quantity	Total Price excl. VAT EUR	VAT	Total Price incl. VAT EUR
Milestone 1 - Hardware	232,786	1	232,786	46,557	279,343
Milestone 2 - Delivery	448,888	1	448,888	-	448,888
Operations and maintenance	14,398	36	518,326	-	518,326
			1,200,000	**46,557**	**1,246,557**

- SITA assumes two payment milestones during the delivery period, to be agreed during the contract discussion.
- SITA's group company SITA BV (Moldova Branch) will act in the capacity of subcontractor for the purposes of procuring and importing of the relevant hardware and equipment. Accordingly, any invoice relating to that hardware and equipment may be issued by SITA BV (Moldova Branch) (and not by SITA Advanced Travel Solutions Limited). The Customer will pay all such invoices. Any such invoice will be subject to Moldovan VAT.

7.4 Security

- SITA takes and implements technical and organizational measures to maintain the confidentiality, integrity, availability and resilience of processing systems and services as well as of the personal data held within such systems. SITA may update or modify these measures from time to time to upgrade the overall security of the contracted services.
- SITA takes measures to guard against unlawful activities which pose a threat to the confidentiality, integrity and availability of SITA customers' data in respect of its provision of any contracted service in accordance with:
  - laws, regulations that are applicable to SITA.
  - industry practices; and
  - the applicable service levels for the relevant services
- SITA employees undergo security and privacy training to ensure they comply with ethical business conduct and can identify security risks and adequately respond to these during their activities.
- SITA manages security incident response activities to minimize any adverse impact to SITA and SITA's customers as well as enable root cause and/or forensics analysis.

8. RISKS, DEPENDENCIES AND ASSUMPTIONS AND ASSUMPTIONS

8.1 Assumptions/Dependencies related to the Delivery/Implementation

8.1.1 Dependencies

ID	Type	Description	Owner	Impact if Delayed or Changed	Mitigation
D1	External	Workflow and Requirements sign-off by Customer, includes specific integration sign-off.	Customer	Increased time for development changes and changes in the configuration and deployment of the gates software by the implementation team. Delay in UAT and sign-off if not documented and sign-off clearly. Risk of scope creep.	Clear requirements and workshop for full explanation of integration requirements. Requirements documented sign-off.
D2	External	Requirements for civil works from the airport expansion project team including locations of gates etc..	Customer	Delay in Civil works and gate installation.	Customer to provide airport expansion plan and cable diagrams at project kick-off and agree to scope from manufactures of requirements for gates installation, cable, power and core drilling.
D3	External	Server room availability for Server install.	Customer	Delay in access to viable server room will delay infrastructure set-up.	Customer to provide details to server room.
D4	External	Acceptance Testing Availability	Customer	Go-live blocked.	Nail down test slots and required participants.

8.1.2 Assumptions

ID	Category	Assumption	Owner	Impact if false	Mitigation Plan
A1	Scope	Workflow, Solution, passport rules and integration signed off by Border Police.	SITA PM	Scope Creep, product work, project acceptance.	Make sign-off a contract deliverable; track as a dependency.
A2	Logistics	Manufacture and Import of all equipment into Moldova can be completed within	SITA PM	Critical Path Delay	Verify customs process and obtain quotes and delivery times from manufacturers to

ID	Category	Assumption	Owner	Impact if false	Mitigation Plan
		the planned lead time			allow for W@R if necessary.
A3	Civil works	Airport will complete power, Network and core drilling. SITA will organise the installation of the gates.	Customer PM and PM	New critical path.	Clear instructions for Airport construction to ensure gates have appropriate civil works for install.
A4	Airport Access	Implementation and Operation teams' access to airports uncompromised - 9-5 Mon to Fri.	Customer PM	Implementation of Servers and software be increased.	Contractual dependency on customer to provide required access or support.
A5	Environments	If the test environment is used, an identical production is necessary to avoid delays.	Customer PM	Any fixes or changes done in test environment may not function correctly in a different Production environment.	Signature of any delay caused by switching environment will be costed as a direct change and will not be subject to delay penalties.
A6	Server Set-up	Access to an office with internet access and workstation for server set-up before installing into server room.	Customer PM	Increased effort to set-up servers once installed in server room	To be discussed during project kick-off
A7	Timely responses	Answers to any technical questions expected within 1 working day.	Customer PM	Day by day slip of integration and development work without timely responses to technical questions	Any main technical contacts to have allocated delegates for the entirety of the project. Solution confirmation discussion at the start of the project.
A8	Hardware Storage and Moving onsite	Hardware is to be stored onsite in a safe place. These are large items which will require a forklift to manoeuvre.	Customer PM	Delay in install if not stored safely and easily moveable.	Ensure and required storage spaces and machinery is available for hardware delivery.

8.2 Assumptions related to support services

To enable the implementation of the Service Model described in this proposal, we propose that the requirements listed here under must be fulfilled by both parties:

- Customer provides SITA support groups, including SITA's Local Subcontractor direct access to the on-premises data centre and any other areas infrastructure is hosted to enable effective faults resolution
- Customer users will report system issues to the SITA Service desk

- Customer will assure local resources ability to resolve issues related to the Components under its responsibility.
- Communication between SITA and support teams is in English
- Customer responsible for local Infrastructure, network, power etc.
- The Customer shall fulfil the responsibilities outlined in the support plan, which will be provided at or shortly after the Effective Date, to enable SITA to meet its obligations.
- Provide designate qualified resources: The Customer will appoint designated employees as the primary Customer contacts. These individuals should be proficient in English, possess appropriate qualifications, and must have successfully completed the training provided by SITA or its authorized third party on Service operation. Designated employees will liaise with SITA, or its authorized third party, for all support activities and oversee solution governance within the Customer's organization.
- Notification of employee changes: Customer is responsible to promptly inform SITA global support of any changes in the designated employees.

Digitally signed by Marinescu Mugurel-Costin
Date: 2025.08.22 16:54:23 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

SITA