AIRPORTS COMPANY
SOUTH AFRICA

Passenger Self-Service Programme

Scope of Work

for the supply, installation and commissioning of Single Token Platform, Automated Border Control (ABC) e-Gates

for Airports Company South Africa

TABLE OF CONTENTS

TABLES

FIGURES

1 INTRODUCTION

1.1 PURPOSE

Airports Company South Africa SOC Ltd hereby invites proposals for the supply, installation and commissioning of a Single Token solution and Automated Border Control (ABC) e-Gates for Airports Company South Africa (ACSA).

This project is a joint initiative between the Department of Home Affairs (DHA) and the Airports Company of South Africa (ACSA).

1.2 OBJECTIVE

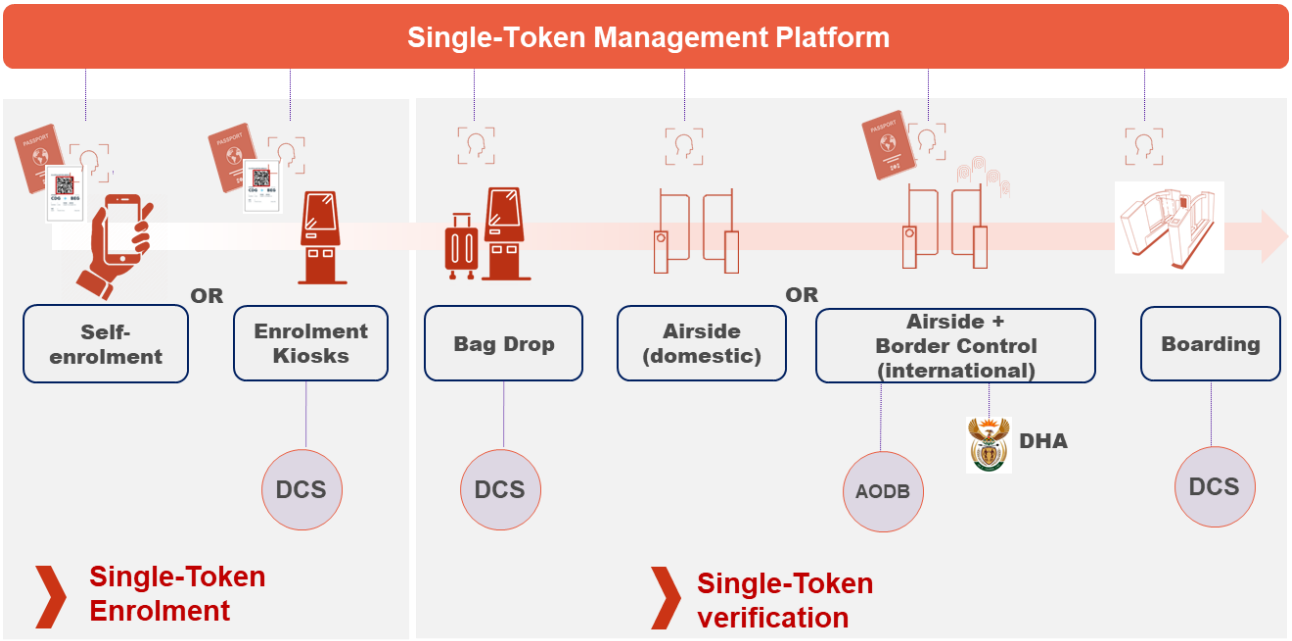
The purpose

The purpose of this Scope of Work (SOW) document is to define the high-level technical and functional requirements related to the supply, installation and commissioning of:

- A Single Token solution to enable an enhanced traveller journey in departures at domestic and international airports. This solution will follow a phased approach as stipulated below, starting with OR Tambo, King Shaka and Cape Town International airport.
- Automated Border Control gates with integration to DHA systems in order to enhance immigration security at international departures and arrivals. This solution will follow a phased approach starting with OR Tambo, King Shaka and Software Support for Cape Town International Airport

The Single Token solution is meant to allow passengers to seamlessly walk through every touchpoint in airports terminals without presenting physical documentation. Instead, their face would be scanned and matched against the initial enrolment authentication - done during enrolment on the ACSA mobile application - or on an enrolment kiosk at the airport. The solution would be used to facilitate automated, self-bag drop, pre-security, immigration and boarding checks in the future, as per the diagram below.

Figure 1. Single-Token usage in passenger departure process



The ABC gates will interface with the Department of Home Affairs (DHA) systems in the execution and automation of the Border Control processes.

The use of automated border control e-Gates has facilitation and security benefits for both ACSA and DHA and these include:

- Processing increased numbers of passengers quickly, conveniently and cost- effectively whilst maintaining the security and integrity of borders
- The automated approach will help to optimize the process and allows resources to be focused on other passengers not being processed automatically, enhanced security using biometrics and improved image can translate into economic benefit and attractiveness to tourists and business passengers.
- On arrivals, the solution would enhance immigration check by providing automated border control (ABC) gates for eligible travellers to be checked against the DHA immigration systems.

Figure 2. Automated Border Control on arrival

ACSA seeks an integrated packaged solution that will meet its core requirements out of the box with minimal modifications. The proposed solution should have a software components, touchpoint and platform which supports biometric algorithm compliant with ISO19794.

The below table indicate the bill of quantities per site:

ITEM	SUPPLY	QUANTITY
1	Single-Token platform - Identity Management Platform license	9
2	Single-Token platform - centralized management	1
3	Enrolment kiosks	12
4	Self-Bag Drop Kiosk	84
5	Domestic airside access gates (DAAG)	24
6	Self-Boarding Gates (SBG)	66
7	Combined Departures Immigration Gates (CDIG)	14
8	International Arrival Immigration Gates (IAG)	10
9	Immigration gates monitoring workstation (IGMW)	4
10	SDK licence for Airport Mobile application for 500.000 users	1

Table 1: Total quantities of equipment to be supplied over a 3-year period

Touchpoints (items 3-7) per airport breakdown is given in the charts below, in a 3 - phased approach

Phase 1 - 2022

Airport	Enrolment Kiosk	Self-Bag Drop Kiosk	Domestic airside gate (DAAG)	Self-boarding gate (SBG)	ABC Combined Departures Gates (CDIG)	Arrivals ABC Gates (IAG)	ABC gate monitoring station
JNB O.R. Tambo International Airport (2 international terminals + 1 domestic)	1	×	×	×	6	4	1
DNB King Shaka International Airport (2 terminals)	1	×	×	×	2	2	1
CPT Cape Town International Airport (2 terminals)	1	×	×	×	×	×	×
Total	3	×	×	×	8	6	2

Phase 2- 2023

Airport	Enrolment Kiosk	Self Bag Drop Kiosk	Domestic airside gate (DAAG)	Self-boarding gate (SBG)	ABC Combined Departures Gates (CDIG)	Arrivals ABC Gates (IAG)	ABC gate monitoring station
JNB O.R. Tambo International Airport (2 international terminals + 1 domestic)	2	32	12	22	6	4	1
CPT Cape Town International Airport (2 terminals)	2	14	6	14	×	×	×
DNB King Shaka International Airport (2 terminals)	2	10	6	10	×	×	1
Total	**6**	**56**	**24**	**46**	**6**	**4**	**2**

Phase 3- 2024

Airport	Enrolment Kiosk	Self-Bag Drop Kiosk	Domestic airside gate (DAAG)	Self-boarding gate (SBG)	ABC Combined Departures Gates (CDIG)	Arrivals ABC Gates (IAG)	ABC gate monitoring station
PLZ Port Elizabeth International Airport	1	8	×	6	×	×	×
GRJ George Airport	1	6	×	4	×	×	×
ELS East London Airport	1	6	×	4	×	×	×
BFN Bram Fischer International Airport	1	4	×	2	×	×	×
UTN Upington International Airport	1	2	×	2	×	×	×
KIM Kimberley Airport	1	2	×	2	×	×	×
Total	6	28	×	20	×	×	×

Phase 4 - Innovation

Phase 4 will be dedicated to innovation in line with ACSA's 4IR strategy and Blueprint. The scope of said phase shall be determined at the end of phase 1 and run in parallel with remaining phases to match and align to ACSA's ambitions towards solving a specific problem, penetrating new markets and introducing new technology.

1.3 Use Cases of the Proposed Solution

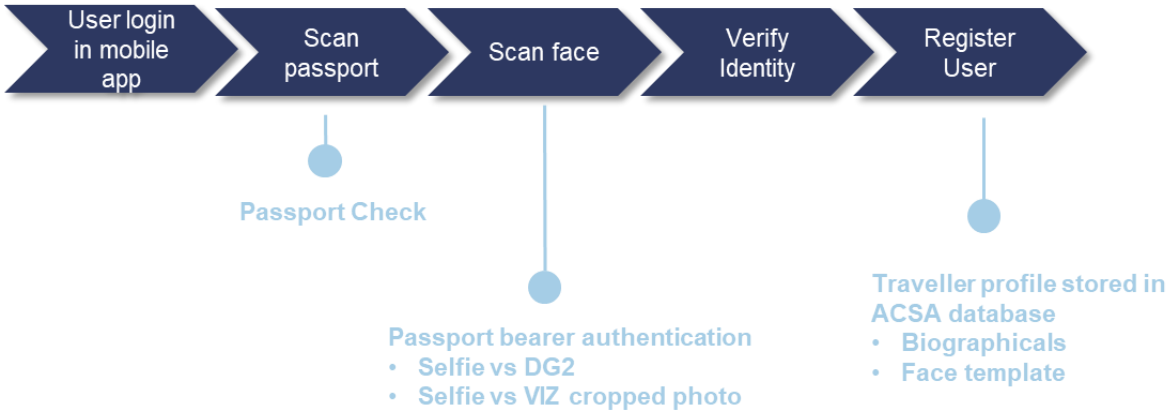
1.3.1 Biometric profile creation with ACSA mobile application

Passengers using the ACSA airport application will create a permanent biometric profile (face and information from traveller's passport) in ACSA database. This biometric profile may be re-used by passengers prior to each travel along with a valid boarding pass to form the single token. ACSA is in charge of developing the airport application by integrating SDKs provided by the bidder. These SDKs provided by the bidder shall provide the following features:

- Passport scan, MRZ and chip data collection (required NFC on the passenger smartphone)
- Extraction of biographical data from the passport (MRZ and DG1 in chip)

- Extraction of passport bearer face from the passport (cropped photo from VIZ and chip DG2 photo when available)
- Passport authenticity check,
- Acquire the passenger live face (selfie) with face image quality and liveness assessment,
- One-to-one biometric comparison between the selfie and the passport face.

Figure 3. Biometric profile creation on ACSA airport mobile application



After creation of the profile, ACSA application stores the following traveller information:

- Passport information
- Face biometric template.

1.4 Single-Token Enrolment

The Single Token solution would allow all passengers to get a biometric token replacing the boarding pass and valid throughout the departure process.

Passengers has two ways of doing the single token enrolment:

- At home, single-token enrolment using the ACSA airport mobile application
- At the airport, using a Kiosk for travellers who are not registered with ACSA or do not want to use the mobile application.

The enrolment process on the mobile application and the kiosks is made available to all passengers whom has a valid travel document (or registered with ACSA airport mobile application) and a boarding pass.

1.4.1 Single-token enrolment on ACSA airport mobile application

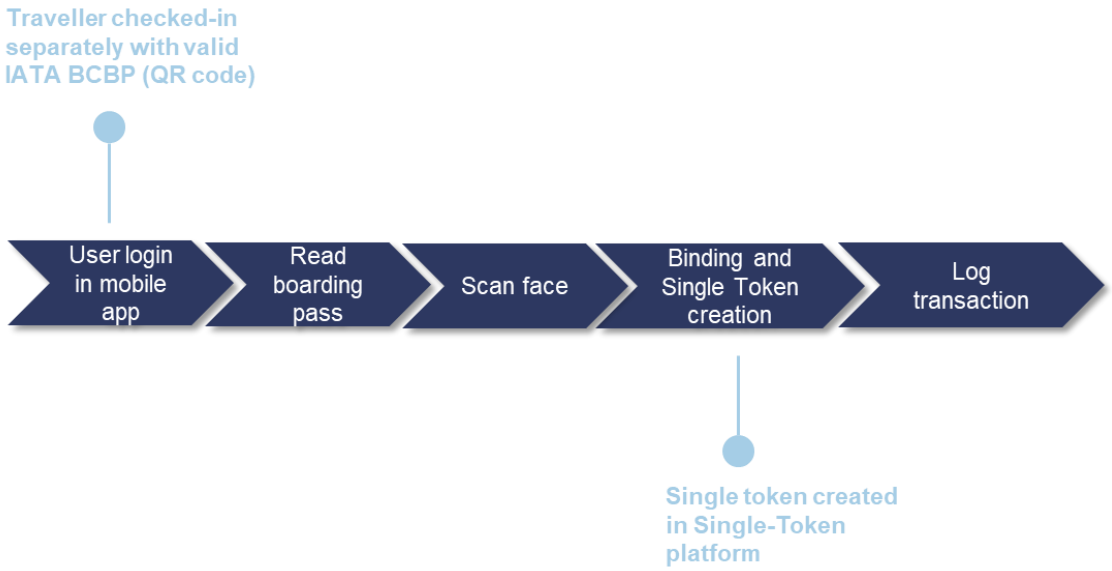
Eligible travellers are already registered with ACSA airport mobile application, have their biometric profile created upfront and have a valid boarding pass after check-in with their airline.

Once logged in in their personal account on ACSA airport application mobile application, travellers will be required to scan their bar-coded boarding pass (obtained on-line through the airline website).

The ACSA application will then associate the biometric template stored along with the biometric profile and the boarding pass. This information will be sent by the application to the Single-Token platform using a Web-service API provided by the bidder, and is called the "binding" process.

To ensure that PDPA / GDPR policies are adhered to, the solution should have a screen to inform passengers on the use, collection and storage of their data as part of the registration process and allow an option to enrol or not enrol.

Figure 4. Single-token enrolment creation on ACSA airport mobile application



After the binding process, travellers can use their single token at all subsequent touchpoints during the departure process.

1.4.2 Single-token enrolment on Self-Service Kiosk at airport

The single-token enrolment is done at the airport using a self-service kiosk, supplied by the bidder (complete hardware and software)

The envisaged process is the following:

- Travellers select the kiosk language
- Travellers scan their valid travel document which is checked (authenticity check)
- Travellers scan their face; a face liveness is performed and a passport bearer authentication is done by comparing the passport photo against the live face acquired
- Travellers scan their valid boarding pass
- The kiosk software initiates the binding process into the Single-Token platform.

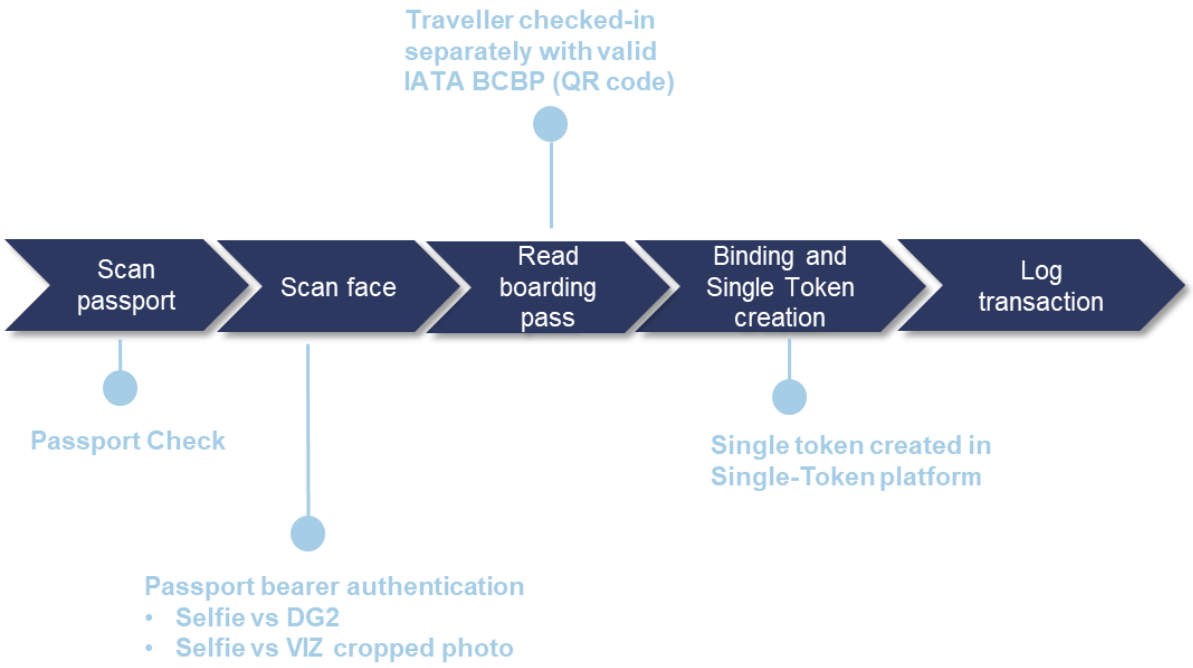


Figure 5. Single-token enrolment creation on the Single-Token enrolment kiosk (STEK)

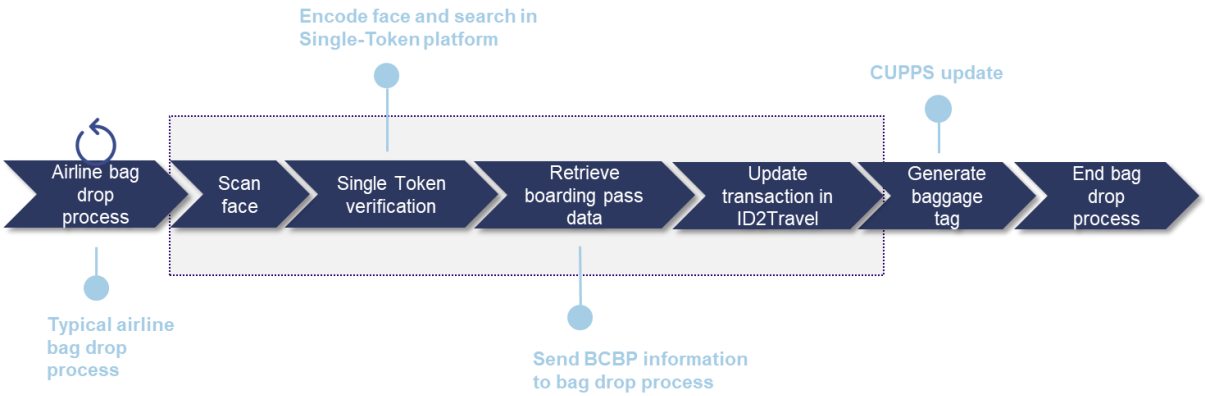
1.5 Self-Bag Drop (SBDK)

Self-Bag drop shall be able to integrate with the Single-Token platform for biometric verification.

The proposed workflow for Self-Bag drop verification is the following:

- Start the bag drop-off using the self-bag drop kiosk touchscreen
- Scan face
- Search for a valid single-token previously bound
- Retrieve boarding pass information from the Single-Token platform,
- Print the baggage tag for the user to stick onto the baggage piece(s)
- Send the baggage to the conveyor

Figure 6. Single-token verification creation at Self-Bag drop



1.6 Domestic Airside access Gate (DAAG) for domestic pre security check

Currently passenger segregation at departure entrance is handled by security personnel who would engage the traveller passenger and authenticate their travel document against the boarding pass and actual facial of the passenger (visual).

The new process will enhance and automate this process.

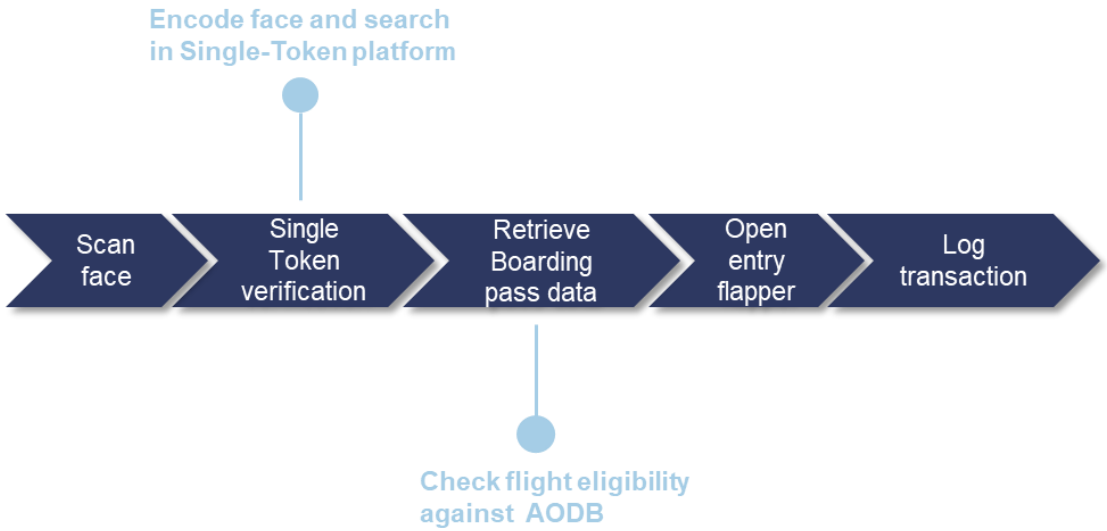
A single-flapper e-Gate with facial biometric scanner would replace the security personnel. Passenger would walk up to the gate and show their face to gain access, the system would then search into the Single-Token platform for a valid token, which is in turn checked against AODB to verify the traveller has an eligible flight.

When all is checks are performed, travellers are allowed to pass through and proceed to immigration or security check.

In the case of a traveller is not authenticated with face after a configurable number of attempts, he will be required to scan his boarding pass as a fall-back measure. If none of these actions enables to find a valid boarding pass for the traveller, he will be directed to a manual process with a security personnel, which needs to remain to handle these exception cases.

The bidder will supply the complete DAAG solution (hardware and software) as well as the integration with the Single-Token platform and AODB.

Figure 7. Single-token verification creation at domestic flight airside access



1.7 International Departures Immigration checks Gates (CDIG)

On international departures, it is envisaged to have an automated, combined airside access and immigration checks.

The CDIG is a dual-door automated gate with a physical mantrap.
At the entry flapper, the traveller would:

- Scan his face
- A valid token is searched in the Single-Token platform, and boarding pass information retrieved
- Boarding pass information is checked against the AODB for an eligible flight

If all checks are successful, the entry flapper would open, and the traveller would walk into the mantrap. In the case of a traveller is not authenticated with face after a configurable number of attempts, he will be required to scan his boarding pass as a fall-back measure. If none of these actions enables to find a valid boarding pass for the traveller, he will be directed to a manual process with a security personnel, which needs to remain to handle these exception cases.
After the traveller has entered and the entry flapper is closed, a check is performed to ensure there is only one person inside the mantrap.

At this point, the immigration checks shall start:

- traveller is required to scan their travel document (passport)
- traveller is required to scan their fingerprints
- Data collected is send to DHA through a DHA-provided web service in order to provide immigration clearance against BMCS (Biometric Movement Control System)

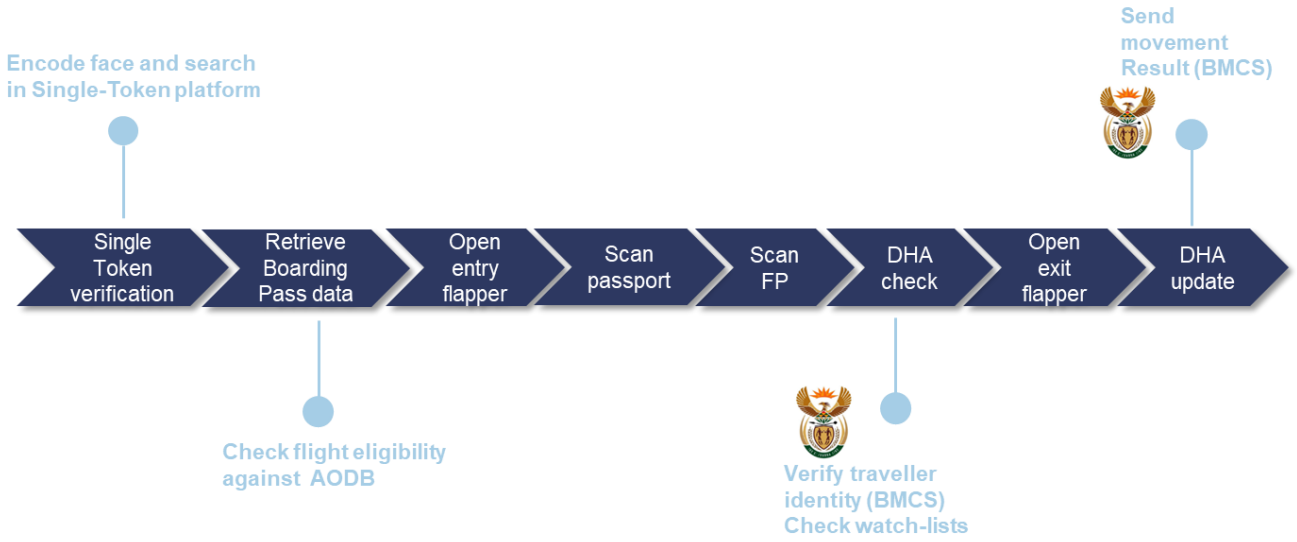
If the traveller is cleared by DHA, the exit flapper opens, and the travellers is invited to leave the mantrap. Once the mantrap is cleared, the exit flapper closes, a message is sent to DHA through a dedicated web service to indicate that the immigration movement is successful, and the CDIG is ready to process another passenger.
In the case of a traveller is not authenticated at the entry flapper through the Single-Token platform, or not cleared by DHA systems, he will be directed to a manual immigration desk.

The bidder will supply the complete DAAG solution (hardware and software) as well as the integration with the Single-Token platform, AODB and DHA systems.

The bidder shall also provide, as part of the solution, an Immigration Gates Monitoring workstation (IGMW), and run by a DHA officer next to the gate. This monitoring station will enable the DHA officer to run and monitor the activity of up to 6 CDIG:

- Activate / deactivate an individual gate
- Display in real-time the overview of the gate status, a detailed information view for each individual gate with the traveller information, check results and exception cases.
- Display the real-time video feed of the mantrap, using a CCTV camera
- The DHA officer can manually solve business exceptions cases (to be defined during the specification stage)

Figure 8. Single-token verification for airside access and immigration checks at international departures



1.8 International Arrivals Immigration Gate (IAG)

On international arrivals, the single token is not used and therefore the bidder is required to only supply an immigration automated gate (IAG).

The IAG is a dual-door automated gate with a physical mantrap. At the entry flapper, the process is the following:

- Traveller scans his passport
- Passport authenticity is checked
- Passport information is sent to DHA systems through a dedicated web service, to determine the traveller eligibility to automated clearance.
- If the traveller is eligible, the entry flapper opens, and the traveller can enter the mantrap

Inside the mantrap, the process continues as follows:

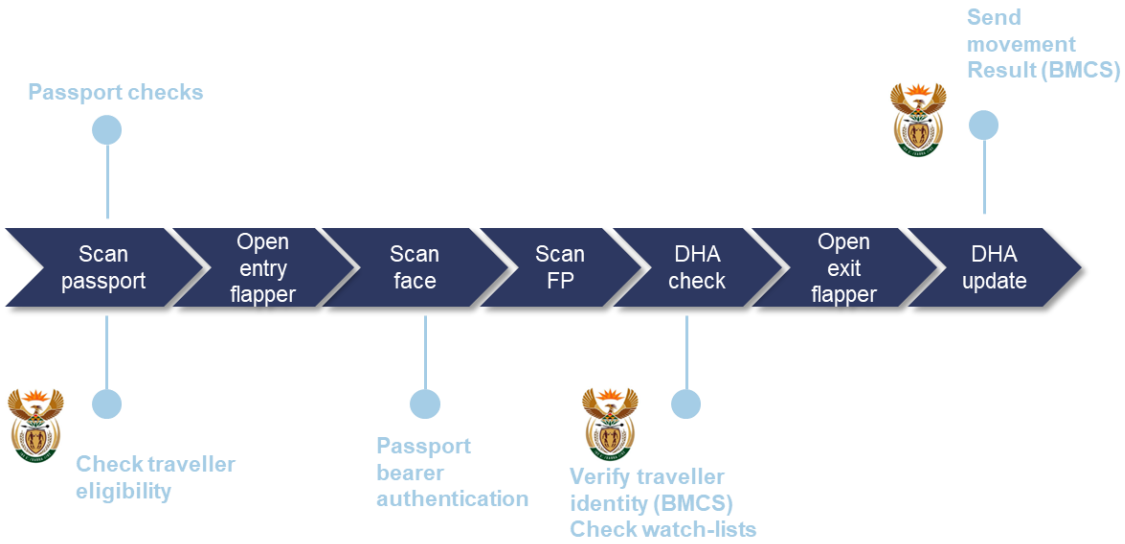
- Scan face
- Passport bearer authentication is done by performing a comparison between the passport photo and live face
- Scan fingerprints
- Data collected is send to DHA through a DHA-provided web service in order to provide immigration clearance against BMCS (Biometric Movement Control System)

If the traveller is cleared by DHA, the exit flapper opens, and the travellers is invited to leave the mantrap. Once the mantrap is cleared, the exit flapper closes, a message is sent to DHA through a dedicated web service to indicate that the immigration movement is successful, and the IAG is ready to process another passenger.
In the case of a traveller is not eligible to enter the gate or rejected by DHA clearance process, he will be directed to a manual immigration desk.

The bidder will supply the complete IAG solution (hardware and software) as well as the integration with the Single-Token platform, AODB and DHA systems.
The bidder shall also provide, as part of the solution, an Immigration Gates Monitoring workstation (IGMW), and run by a DHA officer next to the gate. This monitoring station will enable the DHA officer to run and monitor the activity of up to 6 IAG:

- Activate / deactivate an individual gate
- Display in real-time the overview of the gate status, a detailed information view for each individual gate with the traveller information, check results and exception cases.
- Display the real-time video feed of the mantrap, using a CCTV camera
- The DHA officer can manually solve business exceptions cases (to be defined during the specification stage).

Figure 9. Immigration checks at international arrivals



1.9 Self-Boarding Gate (SBG)

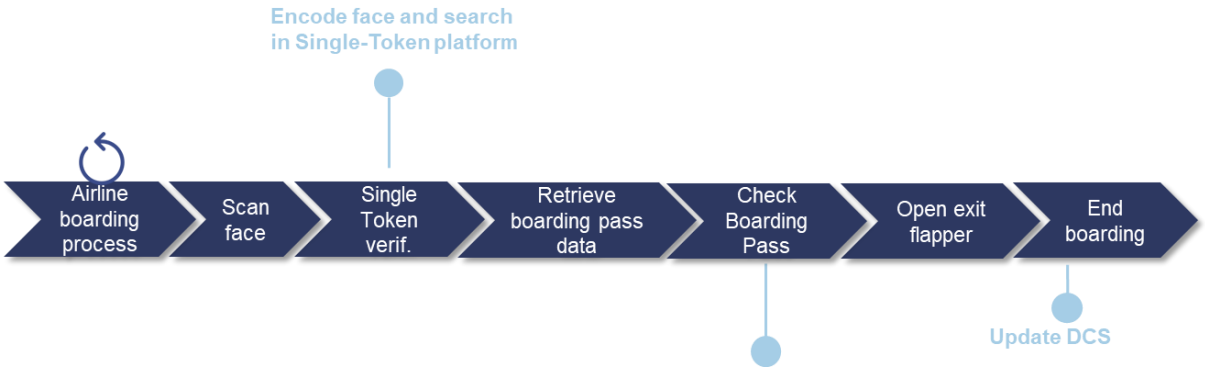
Currently travellers walk up to the boarding gate and the airline agents would view their travel document and scan their boarding pass and scan their boarding pass to allow access.

With the supplied proposed Single-Token solution, the boarding gate would be fitted with a Self-Boarding (SBG). The SBG shall a single-door gate for which the boarding process is the following:

- Scan his face
- A valid token is searched in the Single-Token platform, and boarding pass information retrieved
- Boarding pass information is checked against the airline DCS
- If all checks are successful, the gate flapper would open, and the traveller would exit the gate. The boarding process is considered complete and the SBG sends a notification to the airline DCS.

In the case of a traveller is not authenticated in the Single-Token platform after a configurable number of attempts, he will be required to scan his boarding pass as a fall-back measures. If none of these actions enables to find a valid boarding pass for the traveller, he will be directed to a manual process with an airline personnel, which needs to remain to handle these exception cases.
The bidder will supply the complete SBG solution (hardware and software) as well as the integration with the Single-Token platform and airlines DCS.

Figure 10. Single-token verification for self-boarding


Encode face and search in Single-Token platform
Airline boarding process
Scan face
Single Token verif.
Retrieve boarding pass data
Check Boarding Pass
Open exit flapper
End boarding
Update DCS

2 SCOPE

2.1 IN SCOPE

The sections below outline the business requirements that the bidder needs to respond to. BR1 in section 2.1 outlines the minimum technical and functional requirements that needs to be complied fully.

BR1.	MINIMUM REQUIREMENTS
BR1.1.	**BR1.1.1.** Experience in implementing a Single Token solution using facial biometrics passenger journey for an airport. **BR1.1.2.** The bidder should have at a minimum: • one major Single Token project deployed worldwide using facial biometrics, • one experimental project using the Single-Token operational concept **BR1.1.3.** The projects in reference here above shall include single-token enrolment on mobile application, self-service kiosks, or Self-Bag drops, and single enrolment verification on self-boarding gates at a minimum. **BR1.1.4.** The bidder shall submit a referral letter from the Airport or Airports, with contactable name, number and e-mail address, for Implementation of a Single Token Solution at respective airports mentioned by the bidder (stating the scope of work, duration, status of the implementation).
BR1.2.	**BR1.2.1.** The bidder is to ensure the proposed Single Token solution can work alongside the existing airport and airlines system which require single token integration to enable seamless passenger flow as per ACSA Single Token Passenger Journey concept. The bidder is to provide a write-up on how this will be done.
BR1.3.	**BR1.3.1.** The proposed Single Token solution should comply to IATA, ICAO and NIST standards and procedures. The bidder is to state how the proposed solution complies with the above. The bidder shall prove its compliance in the latest NIST face recognition identification benchmark (FRVT 1:N Identification (nist.gov)) **BR1.3.2.** The bidder shall prove its participation and or compliance in the latest NIST face recognition paperless travel benchmark (FRVT Paperless Travel (nist.gov)) along with the results. The bidder shall confirm its company ranking in this

	benchmark, with a False Non-Identification Rate (FNIR) < 1% on the 1:42000 paperless travel use case.
BR1.4.	**BR1.4.1.** The solution should provide proper disclosure, consent, and opt-out requirements, as well as pay attention to this increasingly complex legislative environment to ensure that biometric data collection and retention is being done in accordance with the national laws. **BR1.4.2.** The solution should be able to capture the best image from single candidate. **BR1.4.3.** Integrates with existing CUPPS and AODB enabling a seamless passenger flow through several types of touchpoints (e.g., Self-Bag Drop, Airside Access, Immigration and Self-Boarding gate. **BR1.4.4.** The Single Token solution should have a capability for a central administration station where remote monitoring or diagnosis can be done to ascertain health and activity of every touchpoint and associated device / peripheral installed. **BR1.4.5.** The solution provided must have a tool to allow to set business rules to change the eligibility criteria, such as nationality and age at the kiosk enrolment. The proposed solution shall consider the user friendliness to configure logic for business rules, models and analysis. **BR1.4.6.** Allow access to only authorised personnel / passenger based on valid and active credentials **BR1.4.7.** For all type of passport, (chip base or non-chip base) the solution should be able to reconcile and verify passenger information and facial profile **BR1.4.8.** The solution should enrol passenger with chip or non-chip passport. The enrolment process proposed in the solution should allow passengers to use any Mobile device (IOS or Android) thru ACSA mobile airport Application when enrolling at home. **BR1.4.9.** The proposed solution must be able, during enrolment at the kiosk, to scan and decipher the data stored within the 2D barcode printed on a paper boarding pass or digitally displayed on the screen of an electronic device **BR1.4.10.** Protection of the data inside and message transmit or received into the Single Token System will need to be ensured. The bidder shall propose and include the necessary protection of data at rest and in motion in order to protect sensitive data manipulated by the Single Token solution. **BR1.4.11.** The proposed solution must be including adequate and up-to-date security patching strategy and virus protection that is to be implemented on the devices, application and Operating System.

	BR1.4.12. The Single-Token platform shall enable to log all transactions performed for audit and business reporting purposes including administrator logins and configuration activities. Logs shall be kept on-line for one year. **BR1.4.13.** The bidder shall Supply, deliver, Install, Test and commission Single Token, complete with the required UPS, power cables, network cables, signal cables, hardware, peripherals, software, integration and services to all airports listed in Section 1, starting with OR Tambo, King Shaka and Cape Town International Airport. The implementation will be rolled over to the remaining airports thereafter.
BR1.5.	**BR1.5.1.** Ensuring at the boarding gate only passenger whom are with valid BCBP (**bar**-coded **boarding pass**) for the particular flight are boarding. Reduces or eliminates slip through. **BR1.5.2.** Passengers do not need to show their travel doc at every touch point, instead use their facial as the ID for access. **BR1.5.3.** The solution shall provide alerts on system and hardware failure and configurable alerts based on reached limits of the defined KPI values.
BR1.6.	**BR1.6.1.** All device and peripheral installed or delivered as part of the total solution should be readily available in the market at least for the next 5 years. In the case it is not, or a newer model is introduced the device should be able to fit into the existing chassis or housing.
BR1.7.	**BR1.7.1.** The bidder shall install the Single Token hardware and peripherals at the locations to be specified by ACSA. **BR1.7.2.** The proposed solution shall include: • Airside Access • Immigration/Emigration ABC gates • Self-Boarding gates • Self-Bag Drop **BR1.7.3.** The bidder is required to supply and deliver other additional devices or material, if there are any, to be used during project work. The bidder shall be responsible for the provision of all necessary tools to complete the project work.

	BR1.7.4. The Single-Token application will run on a virtualized environment provided by ACSA, and or will be hosted by ACSA's IT infrastructure (including all networking and security components) if ACSA choose to host the application and run the workloads though cloud provider/s infrastructure the solution should be capable to be hosted in the cloud. **BR1.7.5.** The bidder shall provide full details of the conceptual design and physical implemented configuration of the proposed solution. **BR1.7.6.** The bidder shall provide full product information of the proposed solution by individual components. **BR1.7.7.** The bidder shall conduct a comprehensive needs assessment to ascertain the needs, wants, desires, operational process and usage patterns of the solution and project. **BR1.7.8.** The bidder shall conduct information gathering with ACSA appointed personnel to ascertain a thorough understanding of the current conditions, current level of service, current processes and desired level of service. In addition, it shall ascertain any existing and/or proposed projects which might influence the system. **BR1.7.9.** The bidder shall Provide Standard Operating Procedures (SOP) for operations and Maintenance as well as day-to-day operations of the system.
BR1.8.	The e-Gates should be able to read chip technology in SA crew member certificates **BR1.8.1.** Until the DHA e-Passport is implemented, chip technology in SA crew member certificates should be used to verify biometrics instead of verifying this against the DHA system. The book format for SA crew members expired in 2011, and was replaced with the polycarbonate crew member card (refer figure 1 below) **BR1.8.2.** The gate must have the ability to read the crew member card, validate it and save the results in a searchable repository

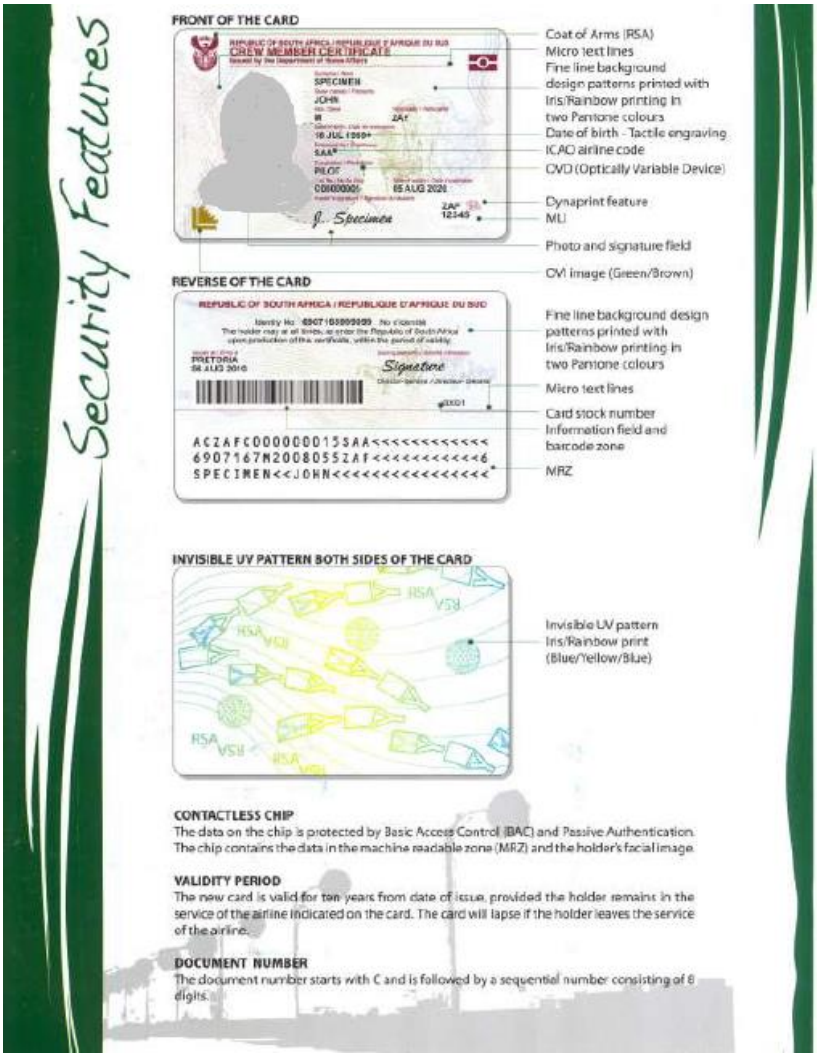


Figure 11: Sample of SA Crew Member Certificate

Table 2: Minimum Requirements

BR2.	SINGLE TOKEN – IDENTITY MANAGEMENT PLATFORM REQUIREMENTS
BR2.1.	**BR2.1.1.** The Identity Management Platform must be compliant to ICAO 9303, IATA and NIST. **BR2.1.2.** The Single Token solution to be deployed must be on IATA CUWS platform once completed. **BR2.1.3.** The application / Solution should work with ACSA's CUPPS provider.
BR2.2.	**BR2.2.1.** The proposed single token software platform should be able to interface with various e-Gate / touchpoints providers. It should not be proprietary to e-Gate or touchpoints. **BR2.2.2.** The proposed solution should allow business administrators to have visibility on passengers that have used any touchpoints installed as part of the project. **BR2.2.3.** The travellers token shall be kept during 24h cycle into the Identity Management system (maximum time) and purged after flight departure as per the applicable legislative prescripts.
BR2.3.	**BR2.3.1.** The Single Identity Management Platform shall be able to search in a full traveller gallery in less than 2 seconds. **BR2.3.2.** The IMP shall have a clear and documented interface in order to be interoperable with 3rd party equipment in the future. **BR2.3.3.** The Identity Management Platform shall be scalable in gallery size and response time. **BR2.3.4.** The system shall be virtualized or containerized as much as possible

Table 3: Identity Management Platform – Single Token Requirements

BR3.	MOBILE AIRPORT APPLICATION SDK AND APIS
BR3.1.	The supplier shall propose an SDK for automatic ICAO identity documents capture (ID1/TD1, ID2/TD2, ID3) and MRZ Optical Character Recognition (OCR) from live video performed by embedded smartphone's camera, running on iOS and Android. Samsung and HarmonyOS, should be catered for within 6-12 months of award. **BR3.1.1.** The following features for this SDK are:

	• Automatic travel document capture • Glare and blur elimination • OCR analysis • Photo cropping and MRZ analysis • Document authenticity check
BR3.2.	**BR3.2.1.** The supplier shall propose an SDK for self-face acquisition by a traveller on smartphone camera, running on iOS and Android (at least 4 OS to be supported within 6 – 12 months). **BR3.2.2.** The following features for this SDK are: • Selfie capture with user guidance and auto positioning detection with user information feedback (too dark, too clear, too blurry) • Photo liveness and anti-spoofing check (Presentation Attack Detection system level 1 and 2 certified ISO/IEC JTC1 30107-3) • 1:1 biometric comparison with the photo extracted from the travel document **BR3.2.3.** The document reader must be able to:

	• Read all types of ICAO-compliant documents regardless of format and design. • Fully compliant with ISO 14443 standard for close range contactless communication • Read an authenticate chips of all ICAO-compliant eMRTD; • The document reader can read the non-chip passport and compare the data on the passport page with the MRZ-data.

Table 4: Mobile airport Application SDK and APIs

BR4.	**Single-Token Enrolment Kiosk (STEK)**
BR4.1.	**BR4.1.1.** The Single-enrolment Kiosk should integrate the following peripherals: **BR4.1.2.** Touchscreen • PC with Application • Passport reader • Boarding pass reader • Camera Facial and Recognition **BR4.1.3.** The kiosk shall be able to implement the workflow described in section 1.3 **BR4.1.4.** The kiosk shall be as compact as possible, easy to use for users between 1m20 and 2m10 (max width 55cm, max height 170cm, max depth 45cm) **BR4.1.5.** Kiosk shall enable to take a face picture of travellers measuring 1m20 to 2m10.

BR4.1.6. Kiosk shall implement the following screens:

- Language selection (min 3 languages)
- Passport reading
- Face acquisition
- Boarding pass acquisition
- Data validation and traveller orientation

BR4.1.7. A solution with a single equipment used for passport reading and boarding pass reading is expected.

BR4.1.8. Kiosk shall present ergonomic screens to guide the user through the different steps

BR4.1.9. At the end of acquisition, data enrolled in the kiosk is sent to the Identity Management platform for single-token enrolment (binding)

BR4.1.10. The full process, for a trained user, shall be executable in less than 30 to 40 seconds

BR4.1.11. Biometric acquisition of face alone shall be executable in less than 4-6 seconds

BR4.1.12. Passport reading and verification shall be fast.

BR4.1.13. The reading time depending on the chip used in the passport booklet, a maximum value is not provided, but comparisons will be made between the different tenderers using different types of passports.

BR4.1.14. Passports usable on the kiosk consists in ICAO-compliant Passports (without chip) and ePassport's (with chip).

BR4.1.15. Verifications of ePassport's shall include as a minimum, in compliance with ICAO Doc.9303:

- PACE (Password Authenticated Connection Establishment) is preferred, or BAC (Basic Access control) if PACE not available,
- Passive authentication,
- Active Authentication (where available)

	• Chip Authentication (where available) • Comparison of DG1 with MRZ, • Verification of expiry date, • 1:1 matching of DG-2 against live face picture **BR4.1.16.** Optical checks of passports shall also be executed, in UV, IR and normal light. **BR4.1.17.** The kiosk ergonomics shall take into account inclusion rules and best practices. **BR4.1.18.** The kiosk shall be able to be used by travellers in wheelchairs

Table 5: Single Token Enrolment Kiosk

BR5.	**SELF-BAG DROP KIOSK (SBDK)**
BR5.1.	**BR5.1.1.** The Self-Bag Drop kiosk shall be able to be integrated on all ACSA bag-drop counters (physical, electrical and network integration), retrofit preferred. **BR5.1.2.** The Self-Bag drop kiosk shall have: • A 15" touchscreen (Minimum) • A status LED • Face capture system with PAD and recognition • Handheld Barcode scanner with lock cable • Integrated Barcode reader • Receipt printer • Bag Tag Printer • Speaker • Intrusion detection sensor • Emergency stop button

	BR5.1.3. The SBDK shall be able to implement the workflow described in **section 1.5** **BR5.1.4.** The Self-Bag drop kiosk shall come with a license for Common Use Web Services connectors **BR5.1.5.** The usage of the SBDK shall be easy, with ergonomic user guidance. Pictograms are preferred to text. **BR5.1.6.** Basic indications such as “Look Here” are allowed. **BR5.1.7.** The SBDK ergonomics shall consider inclusion rules and best practices. **BR5.1.8.** The SBDK shall activate the face camera without traveller action. In case the traveller token is not found in the Single-Token platform, the SBDK shall use the boarding pass reader as a fall-back **BR5.1.9.** The SBDK shall be able to be used by travellers in wheelchairs

Table 6: Self Bag Drop Kiosk

BR6.	**FACIAL AND FINGERPRINT CHARACTERISTICS**
BR6.1.	**BR6.1.1.** The proposed solution and facial biometric camera shall comply with IATA, ICAO and NIST standard and policies. Bidder shall provide best practice and standard for product proposed. The bidder shall state all their product specification but not limited to below. **BR6.1.2.** The camera should be able to perform passive Presentation Attack Detection level 1 and 2 certified ISO/IEC JTC1 30107-3. The detection should not require any specific action / behaviour from the passenger such as open mouth, blinking eyes, etc. **BR6.1.3.** The solution should be able to operate without additional lighting in an environment with ambient light > 400 LUX. **BR6.1.4.** Face acquisitions systems without moving parts are required on touchpoints (bag drop and gates), preferred at the enrolment kiosk. **BR6.1.5.** Face acquisition systems should not exceed 70db noise level in order to be used in airports environments. Silent systems are preferred (ISO 9296) **BR6.1.6.** The bidder is to propose a solution which is able to do the followings in accordance with international border control standard. The bidder shall submit all but not limited to the following specification: • The matching accuracy

	• The face detection time • False Rejection Rate • False acceptance rate • Failure to Enrol Rate • Minimum distance for passenger detection from camera **BR6.1.7.** The bidder must present the performance indicators (False Positive Identification Rate FPIR/False Negative identification Rate –FNIR) of the proposed biometric matching engines for Face matching **BR6.1.8.** The solution should be capable of doing both 1:n and 1:1 recognition / matching mode. **BR6.1.9.** The solution should be able to capture passenger facial for traveller's height between 1.2 m and 2.1m, with a capture distance from 0.4 to 1.3m. **BR6.1.10.** The quality of the facial picture acquired for enrolment shall enable to reach the target FPIR/FNIR. The provider shall explicit the minimum face quality criteria measured in the enrolment solution (from ISO/IEC 19794-5). **BR6.1.11.** The quality of the facial picture acquired for traveller's identity verification shall enable to reach the target FPIR/FNIR. The provider shall explicit the minimum face quality criteria measured for verification (from ISO/IEC 19794-5). **BR6.1.12.** Facial images shall be acquired in less than 7 seconds at the enrolment kiosk and 2 seconds max in verification on other touchpoints. **BR6.1.13.** The facial acquisition device shall have the following certifications: IEC CB, CE, FCC, BIS, RoHS, WEEE **BR6.1.14.** The facial acquisition device shall be available in the form of a stand-alone device or an OEM kit for integration into self-service touchpoints. **BR6.1.15.** The facial acquisition stand-alone device shall have a touchscreen < 10" for passenger display. **BR6.1.16.**
t\]	**BR6.1.17.** The fingerprint verification units should comply to the FBI standards or equivalent. **BR6.1.18.** The fingerprint verification units should support contact 4 finger, fingerprint scanner 500dpi (inside mantrap), with anti-spoofing capabilities, FBI IAFIS IQS Appendix F certified, IP54, with USB 3.0 and USB 2.0 ports. Where a digit is missing, the next available digit should be used, or equivalent standard on FBI IAFIS IQS

	BR6.1.19. The fingerprint verification units should be able to verify two thumbs simultaneously to expedite verification and make it more accurate. Where a digit is missing, the next available digit should be used. This is in line with Dept. of Home Affairs requirements. **BR6.1.20.** The e-gates solution must support multimodal biometrics. At the minimum the e-gate must have facial, and fingerprint (contact) biometric scanners installed. **BR6.1.21.** The proposed e-gates should be able to incorporate future biometric verification capabilities, such contactless fingerprint or iris recognition.

Table 7: Facial and Fingerprint Characteristics

BR7.	**TECHNICAL SPECIFICATION *(ABC eGates)*** **International Departures Immigration checks Gates (CDIG)**
BR7.1.	The following are specific **hardware / software** specifications: **BR7.1.1.** The ABC e-Gates should have the following minimum components. **BR7.1.2.** The CDIG should have two flappers and a mantrap with:

	• Facial Camera with recognition (entry door) • Boarding pass reader (entry door) • Display for traveller guidance (entry door) • Passport scanner (inside mantrap) • Display for traveller guidance (inside mantrap) • Contact 4 finger, fingerprint scanner 500dpi (inside mantrap), with anti-spoofing capabilities, FBI IAFIS IQS Appendix F certified, IP54, with USB 3.0 and USB 2.0 ports. Or Equivalent to FBI IAFIS IQS Appendix F • Emergency button (inside mantrap) • CCTV camera to monitor the mantrap **BR7.1.3.** The CDIG shall be able to implement the workflow described in section 1.7 **BR7.1.4.** CDIG shall be made of stainless-steel casing of 1.5mm thickness minimum, and able to withstand impact of wheel chair and baggage/trolleys accidental impact. **BR7.1.5.** CDIG shall have 1 m high moving and fixed obstacles (at a minimum) tempered glass **BR7.1.6.** CDIG shall not be more than 3000mm long. **BR7.1.7.** The CDIG should be user friendly interface with integrated digital display to allow users/passengers on how to proceed. Additional user guidance in the form of Red and Green LED should be visible to the users/passengers. The gate should provide an intuitive and self-explanatory user interface to inform the passenger step by step how to use the device and avoid any confusion.
BR7.2.	**BR7.2.1.** There should be a sensor in CDIG to ensure that only one passenger passes through one gate at any one time, sensors should alert for any tailgating or un-authorize access/intrusion. The detection system is a fully embedded detection

	system inside the gate cabinet at floor level. The sensor in CDIG should be able to differentiate between passenger bringing a hand carry luggage and tailgating. **BR7.2.2.** The CDIG exit doors must be autosensing for objects or passengers forcing or blocking its movement, and trigger notifications in these occurrences. The exit flappers must not open manually except with the intervention authorize personnel. **BR7.2.3.** The CDIG Sensors shall ensure personal safety and shall adhere to standards and guidelines relating to pinch and shear points of the sensor barrier (European Machinery Directive 98/37/EG or similar) The CDIG shall ensure the following functionalities: ` sensor, Passage sensor, Opposite direction sensor & Safety sensor **BR7.2.4.** The CDIG should have safety sensors which would prevent any injury to passenger. **BR7.2.5.** The CDIG and the used materials should be designed in such a way that it will not be hazardous for a passenger or employee using it. **BR7.2.6.** The used materials for CDIG are vandal proof, scratch resistant, resistant to ultraviolet radiation and resistant to acid, chemical and cleaning product It should also be antistatic. **BR7.2.7.** The CDIG flappers should be transparent and space saving design which allows maximum utilisation of space during installation. **BR7.2.8.** The proposed CDIG should be able to incorporate future biometric verification capabilities, such as facial, fingerprint or iris recognition, as well as intelligent video surveillance of tailgating or left-luggage detection. **BR7.2.9.** The CDIG should be able to operate 24x7 and has a MTBF of minimum 5,000,000 cycles or better **BR7.2.10.** The CDIG shall have a MTTR of maximum 30 minutes. **BR7.2.11.** The CDIG shall be IP40 rated. **BR7.2.12.** The CDIG should operate under 220V power standard and has a UPS back-up of 10 minutes to cater for power failures and run-on building generator system. The e-Gate should be able to withstand power fluctuation. **BR7.2.13.** The CDIG should operate on Low Energy Drive to minimize power consumption. In case of power failure, the gate shall be able to terminate the on-going traveller transaction. **BR7.2.14.** For ease of support the CDIG should be able to be monitored from a central location for its health and system functionality. The admin station / central monitoring station would also be able to do remote diagnosis on a particular e-Gate.

	BR7.2.15. The CDIG shall be installed in banks and easily expandable for additional lanes as and when required when needed with minor connection to the existing lanes. **BR7.2.16.** On each location, at least one CDIG lane shall accommodate PRM travellers. **BR7.2.17.** The CDIG shall have a Mechanical locking system of exit door in case of power failure **BR7.2.18.** The CDIG shall integrate with the AODB for flight eligibility check.

Table 8: *Technical Specification for International Departures Immigration checks (ABC e-Gates)*

BR8.	**DOMESTIC AIRSIDE ACCESS GATE (DAAG)**
BR8.1.	**BR8.1.1.** The DAAG should have: **BR8.1.2.** 1 flapper • Facial Camera with recognition • Display for traveller guidance • Boarding pass reader **BR8.1.3.** The DAAG shall be able to implement the workflow described in section 1.6 **BR8.1.4.** The DAAG shall provide tailgating to prevent multiple persons to use the gate, using a fully embedded detection system inside the gate cabinet at floor level. **BR8.1.5.** The DAAG shall use activate the face camera without traveller action. In case the traveller token is not found in the Single-Token platform, the DAAG shall use the boarding pass reader as a fall-back **BR8.1.6.** The global duration for a traveller between the face scan and the opening of the flapper shall be < 5 s when all checks are successful. **BR8.1.7.** The usage of the DAAG shall be easy, with ergonomic user guidance. Pictograms are preferred to text. **BR8.1.8.** Basic indications such as “Look Here” are allowed. **BR8.1.9.** The DAAG ergonomics shall take into account inclusion rules and best practices. **BR8.1.10.** The DAAG shall integrate with the AODB for flight eligibility check.

	BR8.1.11. On each location, at least one DAAG lane shall accommodate PRM travellers. **BR8.1.12.** The DAAG should embedded the detection system inside the cabinet of the gate at the floor level **BR8.1.13.** The DDAG shall have a Mechanical locking system of exit door in case of power failure

Table 9: Domestic Airside Access Gate (DAAG)

BR9.	**IMMIGRATION GATES MONITORING WORKSTATION (IGMW)**
BR9.1.	**BR9.1.1.** A solution must be provided to monitor ABC immigration gates (CDIG and IAG) **BR9.1.2.** ABC gates monitoring application can only be accessed after successful authentication of the officer **BR9.1.3.** A monitoring officer can supervise up to 6 ABC gates. **BR9.1.4.** An equipment can only be monitored by 1 officer at a time **BR9.1.5.** The monitoring solution shall enable to see in real time the data acquired on the ABC gates and the results of verifications made. **BR9.1.6.** The monitoring solution shall enable a different set of actions for ABC gates **BR9.1.7.** The monitoring solution shall enable to command the opening of the exit doors. **BR9.1.8.** The monitoring solution shall enable to overrule the results of the check for a traveller **BR9.1.9.** The monitoring solution shall enable to display a summary of controls in progress on the monitored ABC gates, and to zoom on one for more detailed information. **BR9.1.10.** The monitoring solution shall be ergonomic and enable to identify quickly alerts raised on an ABC gate. **BR9.1.11.** The monitoring solution shall be available in English language.

BR9.1.12. **Table 10:** Immigration Gates Monitoring Station (IGMS)

BR10.	**INTERFACE / INTEGRATION**

BR10.1.	**BR10.1.1.** The platform should be service oriented. It should be able to consume the internal services using industry standard integration best practices like web services, messaging etc. **BR10.1.2.** The proposed Single-Token solution should be capable of exposing APIs to send and receive data for other activities, for instance enrolment from airport mobile apps, verifying passenger enrolment. **BR10.1.3.** The solution should assure interoperability with other systems by retaining the raw form of any captured biometric in addition to any template derived from the application of a chosen algorithm to the raw form. **BR10.1.4.** The solution shall integrate with: • Airport AODB (DAAG, CDIG) • DHA Web services for traveller clearance (CDIG and AIG) • Airlines DCS for boarding pass validation (SBG) **BR10.1.5.** The proposed solution should allow ACSA to have visibility on travellers processed by the Single-Token platform at the touchpoints installed as part of the project: • Check traveller enrolment status in the Single-Token platform (using traveller's biographical) • Check traveller status across touchpoints within the last 24 hours (using traveller's biographical). **BR10.1.6.** This information must be made available via web based and can be viewed by the Airline agents at the boarding gate for that passenger's flight. **BR10.1.7.** The solution shall offer easy and economic data and system integration capabilities to integrate data into other systems as dashboards, operational control systems etc., ideally via Web Services or on the database level **BR10.1.8.** The bidder shall be responsible to manage and coordinate the integration services which is required as part of total solution. **BR10.1.9.** The bidder shall be responsible for integration to pre-security gates when available for operation.

Table 11: Interface/Integration

BR11.	**REPORTING**
BR11.1.	**BR11.1.1.** The Single Token should be able to produce reports which contain, but not limited to, passenger information and any other information which would enable ACSA to do a complete passenger profiling. All information data transferred or shared or stored should follow the South African Data Protection **BR11.1.2.** Generate reports by Airline, touchpoints, flight, by nationality, by gender etc. All data and integration of data should not contain any traveller's personal data. **BR11.1.3.** The solution shall provide real-time dashboards showing Single Token performance and all peripherals performance. **BR11.1.4.** Dashboard style reports which display data by hourly, daily, by flight etc. **BR11.1.5.** The solution shall be able to create/generate customer-specific reports in xls, .doc, .ppt and.pdf format. **BR11.1.6.** The proposed solutions should have dashboard base reporting which analyst should include, but not limited to the below: • Average number of travellers enrolled in the Single-Token platform per day • Average number of positive matches on a given touchpoint, or a collection of touchpoints (time range) • Average number of negative matches on a given touchpoint, or a collection of touchpoints (time range) • Average number of travellers verified on a given touchpoint, or a collection of touchpoints (time range) • Traveller's nationality, age and gender breakdown on a given touchpoint, or a collection of touchpoints (time range) • Average time to process travellers on a given touchpoint, or a collection of touchpoints (time range)

Table 12*:* Reporting

BR12.	SECURITY REQUIREMENTS
BR12.1.	**BR12.1.1.** The system must go through a vulnerability assessment and penetration testing (VAPT) by a service provider appointed by ACSA. It shall include the server, web application, the API endpoint, the API client, and any other application propose by the bidder for the purpose of Single Token. All issues arise from the VAPT must be resolved in the project timeframe before go-live. The VAPT must be done on the production site. Running a penetration test on a UAT environment is not acceptable as a proof of passing production test. **BR12.1.2.** Any RESTful API must be designed with an authentication framework in mind The bidder may propose any standard authentication method that is suitable **BR12.1.3.** On the selection of standard for the RESTful API, the Bidder may recommend the best method that suits the requirement. The bidder is obliged to secure the transmission of the information over the API. **BR12.1.4.** In any case the bidder required an SSL cert, ACSA shall provide a wildcard SSL cert. **BR12.1.5.** The bidder to ensure the system must incorporate a secure design. For example, only the UI server is allowed to sit on the DMZ and to be protected by ACSA's Web Application Firewall (WAF). Application and database server should be in internal server segment **BR12.1.6.** The solution shall have a documented technical design and operating procedures **BR12.1.7.** The solution shall have a documented technical design and operating procedures **BR12.1.8.** The solution shall be supported by sufficient Hazard Analysis to demonstrate that the introduction of the Single Token process does not increase any operational risk, or any increase in risk to the operation remains tolerably safe. **BR12.1.9.** The solution shall be protected from security threats to a sufficient level, in line with cross-industry standards for internet facing, operational and safety critical systems. **BR12.1.10.** The solution shall be protected from security threats to a sufficient level, in line with cross-industry standards for internet facing, operational and safety critical systems. **BR12.1.11.** The solution shall be designed with industry standard cyber security protection.

	BR12.1.12. The solution shall prevent unauthorised access to the system and the systems it interacts with. **BR12.1.13.** The bidder shall at its own cost, provide a documented cyber security Penetration test report performed by an appropriate organisation, The validation shall be done in less than six months (6) months from the date of final acceptance. **BR12.1.14.** All data stored need to be audited and bidder to ensure it is as per data privacy policy auditing. **BR12.1.15.** The Passenger Data / Information should be encrypted before it's stored and/or transmitted. The data layer should be encrypted. The server where Passenger Data / Information data is stored should be encrypted. The storage disks should be encrypted. **BR12.1.16.** All data should be transmitted using secure transmission method with industry standard. **BR12.1.17.** Data management should be compliant with international directives on Data Privacy Protection.

Table 13: Security Requirements

BR13.	PROJECT MANAGEMENT
BR13.1.	**BR13.1.1.** The bidder shall provide Project Management services to ensure the project properly managed and will meet the timeline. The Project Manager will communicate directly with ACSA internal Project Manager appointed to handle the project. **BR13.1.2.** The bidder shall provide detail project implementation scope and plan, clearly indicating roles and responsibilities, and the key project milestones with timing. The implementation plan should consist of timeline, resource, h/w installation, testing and commissioning and go-live **BR13.1.3.** Propose a schedule for implementation which includes delivery, installation, testing, training and commissioning. **BR13.1.4.** The bidder shall provide the organization chart and project implementation organization chart which define competency level and roles and responsibility at all organization level. (Management level & Proposed site team **BR13.1.5.** As part of the project management approach, the Vendor shall submit a proposed governance structure, including the required meeting formats. **BR13.1.6.** The bidder is to ensure and responsible to specify, supply, install and test the configuration of software and hardware needed inclusive of servers, workstations, Application Software, databases and integration works of every component and subsystem component **BR13.1.7.** The bidder is to manage and conduct full course of training covering the operation and maintenance aspect of the proposed system for the System Administrator. **BR13.1.8.** Managing the stakeholders involved in the project and ensure all issues and escalations are considered for the success of the project **BR13.1.9.** Ensure that meetings are conducted to update project progress to the client as well as stakeholders who are directly involved in the project. **BR13.1.10.** Provide project progress reporting to ACSA's nominated supervisor on timely manner at a bi-weekly frequency including Monthly steering committees **BR13.1.11.** Ensure that all user requirements are captured, and implementation is as per agreed and signed off by ACSA. **BR13.1.12.** Ensure strict adherence to project timeline and all approvals which are required from any parties to be given for consent at least 10 working days in advance.

	BR13.1.13. Bidder is to ensure operational matters are considered when planning for the implementation. As this is a live airport all work and activity needs to be in accordance with security and operational timeline and terms. **BR13.1.14.** The bidders shall provide a valid business registration document and their quality assurance and change management manuals. **BR13.1.15.** The bidder proposal shall be submitted for approval: • Comprehensive implementation plan during development period that ensures no interruption, damage to the existing system • Comprehensive operational contingency plans during the construction and implementation period. The bidder must ensure that there will be no disruption occur during this period. **BR13.1.16.** The bidder shall provide ACSA with Project Implementation & Quality Assurance Plans, detailing the tasks and timelines. The project plan should be in MPP format. **BR13.1.17.** The bidder shall provide all deliverables such as system architecture and design, interface specifications, requirements documents, etc. and shall be signed off by ACSA **BR13.1.18.** A Test Strategy and a Test Plan must be provided by the bidder, including the actual test cases and detailing the composition of the test team. **BR13.1.19.** The testing strategy shall accommodate a minimum of the following test phases: 1. Functional Component testing by testing team in a TEST environment. 2. Functional System Integration testing in the TEST environment 3. Functional End-to-End User testing in the TEST Environment 4. User Acceptance Testing in the UAT environment, with integration with the external systems (CUPPS, AODB, DHA).

Table 14: Project Management

BR14.	TRAINING
BR14.1.	**BR14.1.1.** The bidder shall submit a comprehensive Training Plan to be approved by ACSA for the system operators and system administrators. **BR14.1.2.** The bidder shall describe the training required or recommended to support the Single Token solution's operation. The comprehensive training sessions shall include, but not limited to the followings for all support levels – 1st level recovery team and expert team (i.e., 2nd and 3rd level): • System Administrator Training • Technical Training • Train-the-trainer **BR14.1.3.** The bidder is to ensure training materials available to all participants. The material should be self-guiding and self-explanatory. **BR14.1.4.** The bidder is to conduct an expert hands-on Single Token solution training (includes all devices, peripherals and software) which also include whole necessary task to support at least 2nd level maintenance and not limited to identify, diagnose, troubleshoot, configure and repair etc. **BR14.1.5.** The bidder shall also provide a detail training schedule. Courses provided shall be inclusive of training plan, syllabus, training materials and supporting documentation. ACSA should be allowed to use the training materials in future to train new staff and not have to pay for the course material. The Intellectual Property Right (IPR) for the course material can remain with the bidder **BR14.1.6.** The training schedule should be included as part of the system going live / operational. **BR14.1.7.** The bidder shall submit to ACSA a training report after every training session as specified in the Training Plan

Table 15: Training

BR15.	MANUALS AND DOCUMENTATION
BR15.1.	**BR15.1.1.** The bidder shall provide comprehensive manuals and documentations on all works, plans, procedures and guidelines in hard copy and soft copy to ACSA. **BR15.1.2.** The Application Software will not be deemed to be operational and complete until it has been thoroughly documented. **BR15.1.3.** The softcopy and hardcopy of the manuals and documentations shall be prepared with high quality media and/or printing to the full satisfaction of ACSA **BR15.1.4.** The bidder shall supply minimum four (4) sets of the manuals and documentations (including softcopy) which required by ACSA for use and in-house future enhancement such as: • System requirement specification including system interface, database diagram and other related documents • System design specification including workflow process for each module **BR15.1.5.** All construction drawings must be fully endorsed and submitted to ACSA for review and verification **BR15.1.6.** Upon completion of the works, the Contractor must submit the plan view of the floor Layout showing all newly installed devices, duly endorsed by a ACSA together with representative from the contractor

Table 16: Manuals and Documentation

BR16.	NON-FUNCTIONAL REQUIREMENTS
BR16.1.	**BR16.1.1.** The bidder shall provide the Single Token solution security to preserve confidentiality, integrity and availability of data and communication between server and its client **BR16.1.2.** The Single Token solution must have high availability and reliability that could support ACSA Commercial Operation with the 24 hours per day, 7 days per week (365 days per year) and 99.5% availability uptime per year. The Single Token solution must be able to withstand the load and demand of continuous operations for an extended period. **BR16.1.3.** The proposed Single Token solution shall conform to GDPR standard, Privacy and Personal Data Protection (PDP) policies. The solution should be built on privacy by design concept. **BR16.1.4.** The Single Token solution shall have the ability for the applications/software and hardware/device to grow and scale over time to

	increase in number of transactions processed and changes in workflow and procedures. The Single Token ID solution shall be rapidly and cost-effectively scaled to meet new requirements. **BR16.1.5.** The Single Token solution shall be an open standard technology whereby any enhancement or upgrading can support backward compatibility. All components shall be independent software modules which capable to meet future expansion and requirements. **BR16.1.6.** The bidder shall provide a system that can be rapidly, and cost effectively scaled to meet new requirement over the years. The system components shall be an independent software module which enables the expandability and modularity in meeting future requirements. **BR16.1.7.** The system will be designed without the need to have specialized staff, high maintenance overhead. In addition, the system shall not result in rigid data and reporting structures. System and module/function configuration and management thereof shall be executable at the administrator and coordinating user level respectively. **BR16.1.8.** The proposed system shall be intuitive and user friendly. **BR16.1.9.** The system shall be designed with an excellent user interface that complies with the Graphical User Interface (GUI) so that it is easy to operate by end-users who have basic computer background. **BR16.1.10.** Single Token platform should have the option of being extended and used in other airports in South Africa manage by ACSA. **BR16.1.11.** The Single Token solution and its associated software/database and hardware and protocols used shall not be proprietary in design. It should be of commercial of the shelf (COTS) and its components are replaceable by third party products. **BR16.1.12.** All costs related to the pre-installation, installation, post installation, dismantle and make-good, for any or all damages done during the whole project, shall be borne by the bidder. **BR16.1.13.** Any modifications and/or alterations to the existing infrastructure are subject to review and approval by ACSA. All services are to be identified by the bidder and any modifications required are to be notified to ACSA before work is performed. **BR16.1.14.** All approvals and permits required for the installation are to be completed and taken from competent authority by the bidder. This should be part of the project timeline and any delays or failure to follow up by the bidder which impacts the completion timeline would be bidder's responsibility.

	BR16.1.15. The bidder shall clear and remove from site all rubbish, waste and superfluous materials including any caused by Sub-Contractor from time to time as it accumulates and on completion of the Works. Site should be left in a clean and orderly condition. **BR16.1.16.** Prior to the Works being offered for hand-over to ACSA, the Contractor shall carry out a joint-inspection with ACSA of the Works to ensure that they are finished in every respect **BR16.1.17.** Upon all defects and omissions having been rectified and/or agreement reached, the Contractor shall inform ACSA of the proposed date of hand-over inspection, this shall then be notified to ACSA own internal departments concerned. Where approval and agreement of ACSA other Committees are involved in handovers and practical completion, the Contractors shall ensure that adequate time has been allowed for all concerned to be notified and arrangements concluded. **BR16.1.18.** All conceptual reconfiguration drawings must be verified / endorsed by ACSA prior to works implementation. **BR16.1.19.** All installation work must comply with the Health and Safety (HS) requirements. **BR16.1.20.** The bidder shall observe all safety precautions throughout the performance of this contract. All work shall be in strict accordance with all applicable Safety and Health any other safety related regulations. The bidder must also identify and understand relevant regulations and the implementations of which must be communicated to the site personnel so that they can implement suitable measure **BR16.1.21.** Proper notification signage shall be made available during replacement work to alert the public on the danger that might be imposed by the works. The writing on the signage must be displayed in English. The message on the signage shall also be presented with a suitable picture for ease of understanding **BR16.1.22.** However, the bidder must take into consideration that due to airport operation requirements ACSA can only handover or surrender the identified areas (“implementation sites”) in stages. The bidder is to ensure minimal or no disruption to operations during installation and commissioning activity **BR16.1.23.** The Contractor is to take all precautions that this is a LIVE AIRPORT and by any means not to disrupt the operations of the airports (where applicable). The Contractor is responsible to any claims by the airlines in the event of any loss due to delay of flights as a result of this disruption caused by the Contractor.

	The Contractor is also responsible to make sure the airport is safe to operate after handing over of the site; after completing each daily work activities **BR16.1.24.** The bidder is required to follow strictly all the airport regulations and requirements while working in the airports, failing which not adhere will be held responsible for any accidents or damaged caused. In addition, with this, the bidder shall be responsible for obtaining the necessary permits for operation of his/her machinery, permit to works (PTW) and passes for his/her workers and/or sub-bidder workers to enter any restricted area of the Airport Authority including charge. The bidder is responsible for obtaining necessary permission each time before entering the work site at restricted areas. The bidder is assumed to have allowed for such contingency in the pricing. The bidder works shall not interfere/disrupt the normal and smooth operation of the airport and its ancillary services. **BR16.1.25.** The proposed solution should comply with the POPIA, GDPR and PDPA data privacy acts which is built on the concept of “privacy by design”. ACSA expects the supplier to perform the related professional services (e.g., implementation, commissioning, testing, training, project management, configure reporting and best practices guidance) in a timely and professional manner using their experience in successfully implementing the Single Token solution at comparable Airports around the world with similar requirements as ACSA's. The proposed solution should be in conformity to ICAO’s 9303 and IATA’s One ID Concept.

Table 17: Non-Functional Requirements

BR17.	**IMPLEMENTATION**
BR17.1.	The bidder should **BR17.1.1.** provide lead-times for all equipment **BR17.1.2.** provide requirements that must be in place prior to deployment **BR17.1.3.** provide an extended three to five (3 to 5) years warranty on all installed equipment starting from acceptance date **BR17.1.4.** submit a detail project plan inclusive of all involved parties (e.g., ACSA, South African Revenue Services, Dept of Home Affairs and other involved stakeholders) for review and ACSA approval before implementation

Table 18: Implementation

2.2 OUT OF SCOPE

The following is out of scope for the service provider, but in scope for the project, as ACSA will ensure that this is delivered by ACSA or through an independent consultant as a dependency on this project

- Minimum Tier 2 Datacentre with available space for rack-based infrastructure
- Minimum 10Mbs link to DHA/SITA datacentre
- Associated IT Cabling Infrastructure (networks, core rooms, wire centres) is a dependency for this project and ACSA IT will provide for such requirements however the bidder is expected to provide all relevant technical details of IT Cabling Infrastructure required to implement and operationalise their proposed solution as part of their response to tender.

3 SUPPORT AND MAINTENANCE

This section describes what support and maintenance entail in general and further describes what preventative and corrective maintenance entails for ACSA. For details on this refer to the SLA document.

3.1 ACQUISITION / IMPLEMENTATION SLA's

- The Implementation schedule (dates, milestones, success criteria etc.), including the escalation process to ensure swift decision-making will be defined in the project kick off meeting. Should such schedule not be agreed to, it is stated that if there is no consensus between the parties and it will affect the validity of the contract.
- This implementation is only for phase 1 however it is required that the service provider provide costing for the entire project scope. Funds will be requested from the relevant committees on an annual basis when required.
- The approved minutes of the kick-off meeting will serve as the agreement by the parties of the service level and penalties
- The approved minutes from the kick-off meeting shall be regarded as an annexure and form part of this agreement
- Where the Service Provider does not meet the implementation dates as documented and agreed by both parties in the kick-off meeting, unless clearly and timeously communicated in writing and the schedule re-baselined by the ACSA project manager, ACSA will notify the Service Provider of breach of service
- The service provider is expected to deliver this project in line with the agreed timelines, milestones and conditions
- The Supplier must propose how to best group features and provide incremental solution development, testing and release plan.

- For each release that misses the scheduled release date, and or is above SIT to UAT defect leakage tolerance, ACSA will withhold 10% of the implementation fee per such release. Defect leakage from SIT to UAT must be less than 10% tolerance limit.
- The solution must be in early life support for a minimum of four (4) months
- The service provider should set up a testing lab. The gate should be installed at a lab environment for testing purposes i.e., testing integration with DHA systems.
- The service provider should provide the extended OEM warranty for three to five (3 to years for the gates and the integration. This should be included in the pricing breakdown.
- Infrastructure for the solution must be aligned to ACSA standards.
- Project management for the solution must be aligned to the ACSA standards.
- Business Analysis for the solution must be aligned to the ACSA standards.

3.2 DOCUMENTATION

The Service Provider is expected to produce detailed and updated documentation including but not limited to the following:

- Technical architecture diagrams.
- Technical Design Specifications.
- System Administration manuals.
- List of modules installed and configured.
- Maintenance report template
- Training manuals.
- Standard operating procedures, module manuals including documentation of specific ACSA module configurations at a point in time.

References

ICAO Doc 9303 : **Machine Readable Travel Documents**

https://www.icao.int/publications/pages/publication.aspx?docnum=9303