



sassa

SOUTH AFRICAN SOCIAL SECURITY AGENCY

SOUTH AFRICAN SOCIAL SECURITY AGENCY

Biometric & IAM (BIAM) System Support and Maintenance Terms Of Reference



[*paying the right social grant, to the right person,
at the right time and place. NJALO!*]

South African Social Security Agency

Head Office

SASSA House • 501 Prodinsa Building cor. Beatrix & Pretorius Streets

Pretoria • Private Bag X55662 Arcadia • Pretoria 0083

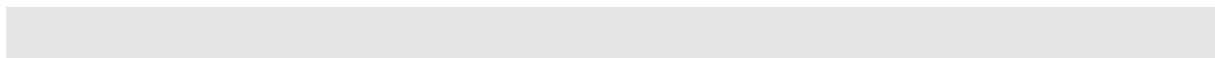
Tel: +27 12 400 2420 • Fax: +27 12 400 2387

www.sassa.gov.za

TABLE OF CONTENTS

SECTION A – OBJECTIVES AND BACKGROUND.....	7
1. OBJECTIVES	7
OBJECTIVES OF TERMS OF REFERENCE	7
2. BACKGROUND.....	7
2.1 BACKGROUND TO THE ORGANISATION	7
2.2 SASSA IMPLEMENTED THE BIAM SOLUTION THAT CONSIST OF THE FOLLOWING COMPONENTS:.....	8
2.3 USAGE OF ORACLE BIAM SYSTEM	8
2.5 SUPPORT AND MAINTENANCE.....	11
SECTION B – SCOPE AND EXTENT OF THE SERVICES	12
3. SCOPE OF THE TERMS OF REFERENCE.....	12
5. PROVISION OF SPECIFIED FUNCTIONS	18
5.1. SERVICES BASE	18
5.2. SPECIFIED SKILLS REQUIRED.....	18
5.3. ADMIN SKILLS WILL BE REQUIRED ON THESE SERVERS/PLATFORMS:.....	19
5.4. CONFIGURATION AND ADMINISTRATION SKILLS REQUIRED FOR OUR SOFTWARE LOAD BALANCER.	19
5.5. NRP ALSO MAKES USE OF THE SASSA MICROSOFT AD BASED CERTIFICATE AUTHORITY.....	19
5.6. NRP ALSO MAKES USE OF JAVACARD TECHNOLOGY FOR BIOMETRIC MATCHING AND ENCRYPTION.....	19
5.7. ORACLE IDENTITY AND ACCESS MANAGEMENT (OIAM) SUPPORT & MAINTENANCE	19
5.8. SOCPEN INTEGRATION REQUIRES:.....	19
5.9. DHA INTEGRATION AND CONNECTIVITY SUPPORT WILL REQUIRE:	20
5.9.2 MS BizTALK SKILLS FOR IJS-BASED CONNECTIVITY.....	20
5.9.3 EXPERTISE IN ESTABLISHING AND MAINTAINING DIRECT API OR NETWORK-LEVEL INTEGRATIONS WITH DHA'S ABIS AND HANIS SYSTEMS.....	20
5.10. ORACLE BIAM SUPPORT FUNCTIONS	20
5.11. DATABASE SUPPORT FUNCTIONS – ORACLE	20
6. LOGISTICS AND TIMING.....	20
6.1. SUPPORT AND MAINTENANCE SERVICES LOCATION	20

SECTION C – EXPECTED ROLES & RESPONSIBILITIES	21
7. SUPPORT.....	21
7.1. ON SITE SUPPORT.....	21
8. EXPECTED ROLES AND RESPONSIBILITIES	21
8.1. SERVICE MANAGEMENT	21
8.2. AUDIT AND HELP-DESK MANAGEMENT	24
8.4. BIAM HELPDESK RESOURCES	27
8.5. TECHNICAL SPECIALISTS.....	27
9. LOCATION FOR PERFORMANCE OF SERVICES.....	29
9.1. ON SITE SERVICES.....	29
9.2. OFFICE ACCOMMODATION AND OTHER FACILITIES.....	29
10. HOURS WORKED AND WORK OUTSIDE NORMAL HOURS.....	30
10.1. NORMAL WORKING HOURS	30
11. RESOURCE REQUIREMENTS: EXPECTED RESOURCES	31
11.1. SASSA SPECIFIC RESOURCE NUMBERS AND LEVELS.....	31
11.2. ALIGNMENT OF SERVICES AND RESOURCES.....	31
12. CONTRACT AND SERVICE STANDARDS	32
12.1. CONTRACT	32
12.2. MEASUREMENT OF SERVICES AND PENALTIES	32
12.3. REPORTING AND COMMUNICATION	33
12.4. VETTING OF ALL BIDDER RESOURCES	33
SECTION D – BID REQUIREMENTS	34
13. SPECIFIC CONTENTS OF THE PROPOSAL.....	34
13.1. BID RESPONSE REQUIREMENTS.....	34
13.2. PREVIOUS EXPERIENCE	34
13.3. RESOURCES KNOWLEDGE AND EXPERIENCE.....	34
13.4. COST BREAKDOWN (PLEASE USE ANNEXURE C TO COMPLETE).....	34
13.5. JOINT VENTURES (JVs)	36



13.5.5.1.	FORMAL JOINT VENTURE - INCORPORATED	36
13.5.5.2.	INFORMAL JOINT VENTURE (NOT REGISTERED) (UNINCORPORATED)	36
13.5.6.	SUBCONTRACTING AND TEAMING AGREEMENTS.....	36
13.5.7.	NO CONSOLIDATED CERTIFICATE.....	37
SECTION E – EVALUATION INFORMATION.....		37
14.	EVALUATION OF THE BID	37
14.0.	BID EVALUATION PRINCIPLES	37
	PHASE THREE: FUNCTIONALITY CRITERIA	38
15.	QUESTIONS AND ANSWERS TO THIS BID.....	41
16.	BID CONDITIONS.....	42

ACRONYMS

Acronym	Description
AD	Active Directory
BBE	Beneficiary Biometric Enrolment solution.
BSC	Business Solution Centre
CEO	Chief Executive Officer
CIO	Chief Information Officer
CFO	Chief Financial Officer
DSD	Department of Social Development
EXCO	Executive Committee
BIAM	Biometric and Oracle IAM system
SRD	Covid R370 Social Relief of Distress Application
SD	System DashBoard (Workflow driven Access Request Web Application)
NRP	Non-Repudiation Program
PIP	Personal Information Profile
PIVA	Person Identification Verification Application
IBM MQ	IBM Message Queue
OGA	Online Grant Application – SASSA web application to apply for normal grants online
SOA	Service Oriented Architecture
HO	Head Office
ICT	Information Communication Technology
IJS	Integrated Justice System
IAM	Oracle Identity and Access Management
MANCO	Management Committee
RO	Regional Offices
SASSA	South African Social Security Agency
SCM	Supply Chain Management

Service Provider	In this document reference to Service Provider also means Bidder and vice versa
Response Template	Microsoft excel spread sheet provided by SASSA to all Bidders to complete with Resources information and costs

SECTION A – OBJECTIVES AND BACKGROUND

1. OBJECTIVES

Objectives of Terms of reference

- 1.1 The main objective of this Terms of Reference is to acquire an all-inclusive on site BIAM Support & Maintenance Service for the South African Social Security Agency for a period of three years.
- 1.2 SASSA requires a comprehensive service which should include any aspect related to support and maintenance for instance any possible application of patches, upgrades, adding new applications to the System Dashboard (Access Request System). Changing/Enhancing the custom programs (Staff Enrolment, Beneficiary Enrolment, Non-Repudiation Program, System Dashboard, Socket server, License management solution, smartcard management solution etc) that is part of the BIAM solution.
- 1.3 Provide professional services to implement the following:
 - 1.3.1 Integration between BIAM and SRD that will allow SRD clients to use the Fingerprint biometric enrolment and verification locally and remotely. Please see point 3.1.2.1 for details.
 - 1.3.1.1 Integration with SASSA systems
 - 1.3.2 Develop a Smartcard Initialisation solution that will allow SASSA to Install SASSA applets on the Smartcard. Please see point 3.1.2.2 for details.
 - 1.3.3 Design, implement, and support an enterprise-grade eKYC (facial biometrics) capability as a shared service. This capability must be consumable through secure APIs by multiple business applications (e.g., SRD, core grants system, and future digital platforms) and must form an integral component of the overall biometric solution.
 - 1.3.4 The eKYC capability must also be securely exposed through internet-facing digital channels to enable grant applicants to perform remote identity verification and authentication as part of the application, review, and servicing processes.

2. BACKGROUND

2.1 Background to the Organisation

As a government entity, SASSA executes an important mandate as part of the service delivery machinery deployed to alleviate abject poverty. In meeting its mandate, it is required to have processes, structures and systems in place to ensure

that the services are delivered efficiently, cost-effectively and to the satisfaction of those who benefit from these services, namely the customer.

2.2 SASSA implemented the BIAM solution that consist of the following components:

2.2.1 The BIAM system consist of an

2.2.1.1 Enterprise-Wide Biometric and Smartcard enabled Oracle Identity and Access Management (IAM) System using Multi-Factor Authentication

2.2.1.2 Non-Repudiation Program (NRP) in an irrefutable and irrevocable manner, link all critical, high impact, and high-risk business transactions to SASSA officials delegated to perform such.

2.2.1.3 A Program (BBE) that Captures and verifies beneficiary fingerprints as part of the enrolment process.

2.2.1.4 License management solution

2.2.1.5 Smartcard management solution

2.2.1.6 Socket server solution

2.2.1.7 Staff Enrolment solution.

2.2.2 Bidders are hereby informed that all custom applications (NRP, BBE, Staff enrolment, Deduplication etc) developed for biometric capture currently utilise

2.2.2.1 Neurotechnology's VeriFinger and VeriLook SDKs.

2.2.2.2 The biometric search capability is implemented using Neurotechnology's MegaMatcher solution.

2.2.2.3 Furthermore, fingerprint matching performed on smartcards makes use of Neurotechnology's Match-on-Card solution.

Any proposed solution must take the above existing architecture and technology stack into consideration.

2.3 Usage of Oracle BIAM system

SASSA went out on tender for the Implementation of a BIAM solution with the following scope of work

2.3.1 Implement an Enterprise-Wide Biometric and Smartcard enabled Identity and Access Control Management System using Multi-Factor Authentication. The IAM

solution must come with automated workflows that will allow the provisioning and de-provisioning of users to be integrated with Oracle System

- 2.3.2 Implementing organizational capability in eliminating fraudulent activities in the Business Systems of the Agency by building a capability to, in an irrefutable and irrevocable manner, link all critical, high impact, and high-risk business transactions to SASSA officials delegated to perform such.
- 2.3.3 Capture and verify beneficiary fingerprints as part of the enrolment process
- 2.3.4 The above three points made up what SASSA calls the Biometric and IAM (BIAM) system.

2.4 Solution Implemented

The Oracle BIAM system was implemented, and it integrates with the following system via connectors i.e. Oracle E-Business Suite, AD and MS Exchange. The following custom programs forms part of the BIAM system.

2.4.1 Employee Provisioning:

When a new employee is added to the ERP HR system, they should be automatically created in ERP, AD and MS Exchange. This capability forms part of OIM and must still be deployed.

2.4.2 Third Party Provisioning:

Third Party consultants follow a different route, because they are not added to our ERP HR tables. A custom program was created to capture the Consultant and that feeds the IAM system to create them on ERP, AD and MS Exchange.

2.4.3 Password Sync between Domain servers and IAM

A Password sync program runs on the Domain controllers to capture passwords when changed and updates IAM

2.4.4 System Dashboard Application

A custom web application that allows workflow driven access request for applications linked into the System Dashboard (ERP, LiveLink, Socpen, BI). This functionality is not live yet.

2.4.5 Non-Repudiation Program (NRP)

Business (currently Socpen and other business applications) identified high risk transactions on Socpen system that must be digitally signed using the NRP

system. When the transaction happens in the source system (Socpen) they must log into the NRP system and approve the transaction by using their fingerprint and Smartcard.

NRP uses public key infrastructure (PKI) to digitally sign identified high risk transactions and then to save it to a secure database.

NRP is a web application that does the following:

- responsible for reading transaction detail (based on the challenge code entered),
- presenting the transaction to the user for approval/rejection,
- integrating with the SmartCard and fingerprint reader,
- generating and signing the hash

2.4.6 VeriFinger and Verilook (NeuroTech) Client Licenses

VeriFinger and Verilook SDK's are used as the fingerprint and facial identification technology. We are using Internet activation option for managing the licenses.

2.4.7 Socket Server Software

The Socket Server is a desktop application that acts as a translator and messenger between the web applications (e.g. NRP, BBE) and the fingerprint scanner. Because web browsers are not allowed to communicate directly with hardware devices like fingerprint scanners and card readers, the Socket Server bridges that gap.

It keeps a secure, always-open line of communication so that when the web application requests a fingerprint, the scanner responds immediately and the result is sent back in real time.

Beyond capturing fingerprints, the Socket Server also:

- Manages on-card matching requests for authentication, ensuring that the person's fingerprint matches what is stored on a smart card.
- Reads and writes (in the case of an enrolment request) to smart cards, supporting secure storage and retrieval of biometric data.

In practical terms, it:

1. Receives instructions from the web application.
2. Communicates with the fingerprint scanner and smart card.

3. Performs verification, reads and writes data on the card.
4. Returns results back to the web application instantly.

Socket server solution was developed using C#

2.4.8 Staff Enrolment Application

This application is used to verify SASSA employees against DHA and enrolls their fingerprints. This system also manages the employee's access to NRP.

2.4.9 Beneficiary Enrolment Application

Is a web application that is used by SASSA staff to capture and enrol beneficiary's fingerprints during the enrolment process. During the enrolment process the beneficiary's identity is verified against DHA's database by making a PIVA service call

2.4.10 Management of Security Certificates used in Non-Repudiation Program

The biometric non-repudiation solution makes use of server-side and client-side certificates.

Server-side certificates are issued by the SASSA Certificate Authority, running on Microsoft AD Certificate Services.

Client-side certificates are issued by the non-repudiation solution vendor.

The successful bidder will be expected to proactively manage these certificates to ensure that SASSA does not experience service interruptions due to expired certificates.

2.4.11 SmartCard configuration

Install required software on the new SmartCards.

The smartcards store biometric data (fingerprint template) and generates cryptographic key pair on-board. The smartcard has a PKCS11 store containing the private key and is locked by the user's fingerprint. The transaction hash is sent to the smartcard where the private key signs the hash (after a successful fingerprint match-on-card has been performed).

2.5 Support and Maintenance

The Implementation of the Biometric Identity and Access Management (BIAM) system has now come to an end. SASSA now seeks to issue a request for a bid for implementation, support and maintenance as per the above services for a period of three years.

SECTION B – SCOPE AND EXTENT OF THE SERVICES

3. SCOPE OF THE TERMS OF REFERENCE

3.1 Required Services

The successful bidder will be expected to execute and conduct the following services / tasks for the Agency for a period of three years:

- 3.1.1 Provide full scale on-site support and maintenance services to the Agency by supporting all Oracle IAM and all related custom applications (NRP, Staff Enrol, Ben Enrol, System Dashboard, BizTalk (IJS connectivity), IBM MQ etc.), and any future new developments, including the users and business users whose work is related to the system or integrates with the system, with effective and efficient direct support and maintenance services which will accrue to the benefit of SASSA Head Office as well as the SASSA Regions, Districts and Local Offices.

3.1.2 Implementation

3.1.2.1 Biometric Verification Integration Requirements

The successful bidder shall redesign the existing BBE application using an API-first approach to expose fingerprint biometric enrolment and verification capabilities as reusable enterprise services. The solution must enable consumption by multiple SASSA business applications and support secure identity enrolment and verification for SASSA clients through both local service points and internet-facing digital channels (remote).

The solution shall expose the fingerprint biometric verification functionality through secure, standardised interfaces (e.g., APIs or services) to authorised systems, including but not limited to the eKYC application and OGA systems.

The modified BBE application shall support controlled access to fingerprint biometric services through appropriate authentication, authorisation, and audit mechanisms.

The solution shall ensure interoperability between the BBE application and other SASSA business applications (eg OGA, eKYC etc) without compromising existing functionality or performance.

All integrations shall comply with applicable security, data protection, and privacy requirements governing biometric information.

The bidder shall ensure that the redesign supports scalability and does not negatively impact current biometric verification operations.

All biometric data must be stored in the central biometric repository with reference to source application.

3.1.2.2 Smartcard Initialisation and Personalisation Requirements

The successful bidder shall design, develop, implement, and maintain a secure smartcard initialisation and personalisation solution. The solution must ensure that each smartcard is uniquely identifiable, securely configured, and cryptographically protected prior to issuance.

The bidder shall meet the following minimum requirements:

1. Software Development Requirements

- Develop a secure smartcard personalisation application.
- Ensure the solution supports secure communication with smartcards.
- Provide comprehensive audit logging of all personalisation activities.
- Ensure integration capability with existing backend systems and databases.

2. Cryptographic Key Management

- Implement secure generation and/or injection of cryptographic keys.
- Integrate with a Hardware Security Module (HSM) where applicable.
- Ensure replacement of all default manufacturer keys prior to activation.
- Enforce secure key handling and storage in accordance with applicable security standards.

3. Application Loading and Configuration

- Load required smartcard applications during initialisation.
- Configure security domains and access conditions.
- Enable secure messaging where required.

4. Card Personalisation

- Load user-specific data onto the card.
- Provision digital certificates where applicable.
- Configure PIN, PUK, and retry counters in accordance with defined security policies.

5. Backend Integration and Registration

- Register card serial numbers and associated credentials in the backend system.
- Link each card to the authorised end user.
- Maintain card lifecycle status (e.g., initialised, active, suspended, revoked).

3.1.2.3 eKYC Design, Implementation, and Support

Context and Strategic Intent

SASSA currently utilizes multiple biometric service providers, resulting in a fragmented landscape where facial recognition is primarily limited to the SRD R350 environment through a third-party electronic Know Your Customer (eKYC) platform. In contrast, core grant administration relies on the custom-built Beneficiary Biometric Enrolment (BBE) web application for fingerprint verification. This fragmentation creates operational constraints, particularly for beneficiaries with poor fingerprint quality, physical impairments, or when accessing remote digital channels.

To address these limitations, SASSA requires a standardized, enterprise-grade eKYC capability. The successful bidder will utilize an API-first approach to design, implement, and support this solution, ensuring it functions as a shared service consumable by multiple business applications such as SRD, the core grants system, and future digital platforms. The solution must also be securely accessible to grant applicants over the internet through approved digital channels, enabling remote identity verification, facial recognition, liveness detection, and authentication as part of grant application, review, and beneficiary servicing processes.

This development must leverage SASSA's existing technical stack, specifically the KrakenD API Gateway for service orchestration and the Java Enterprise Edition (JEE) API layer for backend persistence. By adopting this

methodology, the bidder will provide facial recognition and liveness detection through secure, standardized APIs that integrate seamlessly with the central biometric repository. The solution must support both internal business applications and internet-facing self-service channels while enforcing appropriate security controls, privacy safeguards, fraud prevention measures, and performance standards.

This approach future-proofs the Agency's architecture by enabling assisted service channels, internal business systems, and digital self-service platforms to access unified biometric verification services through a common enterprise capability, without compromising performance, scalability, security, or user experience.

1. Architectural Requirement: API-First eKYC Service

- The successful bidder must develop the eKYC (Facial Biometric) solution as a standalone, decoupled microservice rather than a module within an existing application.
- Decoupled Logic: The facial capture, liveness detection, and verification logic must reside in a dedicated API layer, separate from the User Interface (UX).
- Universal Accessibility: The service must be accessible to all SASSA business applications—including Socpen, SRD, ERP, and future OGA systems—through the centralized KrakenD API Gateway.

2. Technical Specifications for the API Layer

- To maintain consistency with the existing BIAM environment, the API-first development must adhere to the following:
- Core Protocol: All eKYC functions must be exposed as RESTful APIs using Java Enterprise Edition (JEE) with JPA persistence for the backend.
- API Management: All eKYC endpoints must be registered, secured, and managed through the KrakenD API Gateway.
- Standardized Documentation: The bidder must provide comprehensive API documentation to allow other application owners to integrate with the eKYC service independently.
- Security and Authentication: The APIs must integrate with the Oracle Access Manager (OAM) for secure token-based authentication (OAuth2/OIDC), ensuring only authorized applications can invoke biometric functions.

4. Functional Scope of the eKYC API

The eKYC API must expose the following capabilities, utilizing the Neurotechnology VeriLook SDK as specified in the technical requirements:

- Facial Capture & Quality Check: An endpoint to receive image data and return a quality score based on defined biometric standards.
- Liveness Detection: A service to verify that the captured face is a live person and not a photograph or spoof.
- 1:1 Verification: An API to compare a live facial capture against the image stored in the SASSA repository or provided by the Department of Home Affairs (DHA).
- 1:N Identification: Integration with the MegaMatcher (MMA) search engine to check if the face already exists in the repository for de-duplication purposes.

4. Integration and Future-Proofing

- Source System Agnostic: The API must be designed to handle requests from diverse platforms, including web-based custom applications (BBE), mobile devices, and legacy mainframe systems via the existing IBM MQ and MS BizTalk integration layers.
- Operational Standards: The solution must ensure scalability, high availability, and performance to support national demand while complying with all applicable security, privacy, and data protection requirements.

PLEASE SEE SECTION 2.2.2 FOR SDK'S CURRENTLY IN USE

4.1.1 The successful Bidder will be required to provide a comprehensive service (in terms of User Support - typical Help Desk services, Functional services, Technical services, System Administrator (user access management), Audit Management services, Programme and Project Management services, Training Services and DBA services) to SASSA for all Business Support and Maintenance services for a period of three years.

4.2 Oracle BIAM Usage

4.2.1 The Oracle BIAM solution consists of Oracle IAM and number of custom developed programs that enable the Staff Enrolment, Beneficiary Enrolment, Non Repudiation Program (NRP), System Dashboard (Access Request system), Verifinger and Verilook SDK (Neurotech) license, Socket server software, Password Sync program

4.2.2 Integration with connectors to AD, MS Exchange, Oracle EBusiness Suite

- 4.2.3 Integration with Socpen (mainframe) for User provisioning (workflow driven access request) using IBM's MQ software.
- 4.2.4 Integration with the Department of Home Affairs (DHA) for PIP and PIVA services. This includes support and maintenance for connectivity through the Integrated Justice System (IJS), direct network connections to DHA's ABIS, direct connections to DHA's HANIS, and any future connection methodologies adopted by the Agency during the contract period.
- 4.2.5 Integration with PostBank
- 4.2.6 Integration with EBusiness Suite, Socpen, LiveLink and MS BI
- 4.2.7 Proactively Manage Client and Server Side Security Certificates to ensure that SASSA does not experience service interruptions due to expired certificates.

4.3 Support and maintenance services for these three years will also amongst others matters include:

- 4.3.1 Support and maintenance of the Oracle IAM and number of custom developed programs that enable the Staff Enrolment, Beneficiary Enrolment, Non Repudiation, System Dashboard (Access Request system), Enrolment of Third Parties (not in ERP HR), Verifinger (Neurotech) license, Socket server software, Password Sync program, Card Apps, Management of Client & Server security certificates, IBM MQ, connectivity to the DHA for biometric verification services (including but not limited to BizTalk/IJS, direct ABIS, and HANIS connections
- 4.3.2 Support and Maintenance after the sub-projects (see 1.3) have been implemented.
- 4.3.3 Upgrades,
- 4.3.4 Maintenance activities eg patching, cloning, Performance Tuning, Backup & Recovery and DR testing
- 4.3.5 24 hour monitoring of Service Requests with Oracle,
- 4.3.6 Assistance with the provisioning of reports and answering of questions to the Auditors,
- 4.3.7 On-going training and skills transfer (either individually or classroom based); etc,
- 4.3.8 Maintaining and storing Custom application source code in a central repository

5. PROVISION OF SPECIFIED FUNCTIONS

5.1. Services Base

The following services form the scope of this terms of reference and will be delivered by the Bidder through the SASSA Business Solution Centre:

- 5.1.1 Service, Programme, Project and Audit Management services
- 5.1.2 Support and maintenance of all Oracle IAM, Staff and Beneficiary Biometric enrolment, NRP and all custom developed Applications that make up the BIAM system.
- 5.1.3 Maintain/Improve current Integrations and Integration with new External Data Resources as they become available.
- 5.1.4 System Enhancements and System upgrades;
- 5.1.5 Integrate new SASSA applications with the System Dashboard ie workflow driven Access Management,
- 5.1.6 Performance tuning
- 5.1.7 Disaster Recovery- and business continuity planning and testing;
- 5.1.8 Continuous update of core training material (incorporating business processes; system processes etc. into one training delivery platform) coordination, (scheduling, enrolments and assessments) support and maintenance thereof on Oracle Learning Management and
- 5.1.9 Ensuring SASSA sustainability in terms of comprehensive training updates, knowledge and skills transfer, implementation and roll-out of existing, new enhancements and upgrades when required.
- 5.1.10 The biometric non-repudiation solution makes use of server-side and client-side certificates. Server-side certificates are issued by the SASSA Certificate Authority, running on Microsoft AD Certificate Services. Client-side certificates are issued by the non-repudiation solution vendor. The successful bidder will be expected to proactively manage these certificates to ensure that SASSA does not experience service interruptions due to expired certificates.

5.2. Specified Skills required

The successful bidder will be expected to provide support and to maintain the following functions as part of the comprehensive inclusive service

General: Deep understanding of the below technologies:

- 5.2.1 Security, Identity and Access management

- 5.2.2 Fraud Prevention and Detection
- 5.2.3 Large Scale Biometrics Standards and Architecture
- 5.2.4 Enterprise Integration Architecture
- 5.2.5 Analytics and Data Science

Technical competency:

- 5.2.6 NRP, Staff Enrolment, Beneficiary Enrolment, Card Swap Apps and the System Dashboard UX layer were developed using the following technologies:
- 5.2.7 Authentication: Oracle Access Manager
- 5.2.8 Frontend: Angular (also requires typescript and javascript skills)
- 5.2.9 API Layer: Java Enterprise Edition, including JPA persistence.
- 5.2.10 Database: Oracle 19c
- 5.2.11 IBM MQ
- 5.2.12 SmartCard

5.3. Admin skills will be required on these servers/platforms:

- 5.3.1 NGINX (Webserver)
- 5.3.2 Weblogic (JEE Server)
- 5.3.3 KrakenD – API Gateway
- 5.3.4 Oracle Linux OS

5.4. Configuration and administration skills required for our Software Load balancer.

- 5.4.1 "HAproxy" load balancer

5.5. NRP also makes use of the SASSA Microsoft AD based Certificate Authority.

- 5.5.1 Admin and integration skills with this platform will be required.

5.6. NRP also makes use of JavaCard technology for biometric matching and encryption.

- 5.6.1 JavaCard development and NeuroTechnology SDK integration skills will be required.

5.7. Oracle Identity and Access Management (OIAM) Support & Maintenance

5.8. SOCPEN Integration Requires:

- 5.8.1 IBM MQ integration (JEE based) skills

5.8.2 IBM MQ Queue Manager configuration and administration skills

5.8.3 Oracle Identity Manager Web Service Connector development skills

5.9. DHA Integration and Connectivity Support will require:

5.9.2 MS BizTalk skills for IJS-based connectivity.

5.9.3 Expertise in establishing and maintaining direct API or network-level integrations with DHA's ABIS and HANIS systems.

5.10. Oracle BIAM Support functions

5.10.1. Service Management

5.10.2. Audit Management

5.10.3. Programme and Project Management

5.10.4. User Support (Typical Helpdesk function)

5.10.5. User access management

5.10.6. Training Management (OLM & UPK)

5.10.7. Technical Services

5.10.8. Application Database Administration

5.10.9. System Administration (incl Weblogic, Nginx, HAProxy, Krakend, MQ, BizTalk)

5.11. Database Support Functions – Oracle

5.11.1 Database Administration

5.11.2 Support and Maintenance Management

5.11.3 Patch Management

5.11.4 Backup and Recovery

5.11.5 DR Testing

5.11.6 Performance tuning

6. LOGISTICS AND TIMING

6.1. Support and Maintenance services Location

6.1.1 50% of the support and maintenance services will be performed on-site from the SASSA Head Office premises in Pretoria and 50% can be performed remotely. Sufficient space, desks and equipment is made available for the Bidder in this regard. Regional support will be provided telephonically, via conferences etc. from the Pretoria location.

SECTION C – Expected Roles & Responsibilities

7. SUPPORT

7.1. On Site Support

7.1.1. SASSA insists on having on-site support services to be provided at the SASSA Head Office in Pretoria and which services will form part of; and slot into the BIAM Business Solution Centre of SASSA. Regional support will be provided from this premise telephonically, through conferences etc. Occasionally, travel might be required to the Regions which cost will be borne by SASSA.

8. EXPECTED ROLES AND RESPONSIBILITIES

8.1. Service Management

The Service Management component consists of a dedicated; on-site service manager (Programme Manager) and Project and administration resources (Project Management Office (PMO) for project management, audit management, quality assurance and configuration management) that will be called on to maintain existing baselines and provide regular status snapshots on conformance and quality adherence.

The Service Manager

The Service Management components include the following roles and responsibilities which includes the development, establishment, implementation and co-management of all of the following aspects:

- 8.1.1. Providing the framework, guidelines and development, of documentation for establishment of service levels between the BSC and other SASSA LOB's (HO and Regions).
- 8.1.2. Definition and implementation of policies and procedures for the Business Support Centre
- 8.1.3. Definition of; enhancement of; and provision of SASSA BIAM system support configuration management standards and procedures.
- 8.1.4. Definition, implementation of system support and version control policies and procedures.
- 8.1.5. Planning and management of system enhancements, (inclusive of monitoring of resource percentage of time allocation on enhancements), system changes, system patches, upgrades, testing cycles.

8.1.6. Establishment of release management policies and procedures.

8.1.7. Resource management and planning:

8.1.7.1. Resource requirements will be driven around system support and system enhancement requests including minor and major system changes. The identification of Business and system process changes and the planning of training and knowledge transfer to key SASSA staff to implement developed and approved changes.

8.1.7.2. Resource management can be summarised in the following categories:

- a. Identifying scope of work
- b. Mapping of scope of work to existing resources
- c. Identifying specific/additional resource needs
- d. Completion of resource schedules and resource plan, inclusive of staffing practices, leave; replacements etc.
- e. Regular monitoring of resource compliment and scope of work.

8.1.8. Definition of the knowledge and skills transfer strategy and plan; implementation thereof and regular monitoring of planned progress against planned activities.

8.1.9. Change Control policies and procedures

8.1.9.1. *Maintenance and enhancement of system change control procedures and policies*

8.1.9.2. *Maintenance and enhancement of BSC change control management forum where necessary*

8.1.9.3. *Management and planning of approved change requests including: requirements definition, system testing, acceptance and implementation*

8.1.9.4. *Identifying of resource required to complete approved change requests.*

8.1.10. Finalising of monthly invoicing, inclusive of:

8.1.10.1. *Identification and tracking of deliverables where applicable; and*

8.1.10.2. *Comprehensive monthly progress and status reports on all application; technical and call management environments.*

8.1.11. Provision a management tool to monitor service requests and consolidate knowledge gained, should the current SASSA systems be unsupportive / not meeting the specific requirements of meeting the BIAM requirements.

Project Management Office – PMO (Administration Function)

The Administration Function components include, amongst others, the following roles, responsibilities and aspects:

8.1.12. Project Management

This includes, but is not limited to; functions such as:

- a. Development of Business Case, with risk and cost management
- b. Development and maintaining of project plans, reports, spending etc.
- c. Ensuring development of training material etc.
- d. Ensuring all project documentation (i.e. functional and technical specifications are developed and maintained)
- e. Ensuring full SDLC cycle is followed
- f. Ensuring all sign-off is obtained etc.

8.1.13. Reporting, Issue and Risk Management

This includes functions such as:

- a. *Business report for SASSA*
- b. *BSC reports (weekly, monthly, quarterly etc.)*
- c. *Issue and Risk Management (development and safekeeping of Risk and Issue logs, Risk memo's, etc.)*

8.1.14. Configuration and other management process

This includes functions such as:

- a. Version control
- b. Release management

- c. Change control
- d. Quality control
- e. Problem and issue management
- f. Specific template development (examples)

8.1.15. BSC Library

This includes the development (where not already in existence), support and maintenance of the following:

- a. Structures and Naming conventions
- b. Standardization and Templates
- c. Procedures and access
- d. Indexing
- e. Intranet usage
- f. Training and test scripts - regular updates

The PMO resources should be able to manage the full SDLC life-cycle of any projects as will be defined from time to time in the BSC. A senior project manager is required and could be supported by other administrative resources.

8.2. Audit and Help-desk Management

8.2.1. The audit manager will be responsible for amongst others the following tasks:

- 8.2.1.1. Ensuring that all monthly audit requirements are attended to;
- 8.2.1.2. Ensuring all monthly audit requirements are documented and signed-off;
- 8.2.1.3. Reviewing all previous audit findings and ensuring that the improvements are implemented and enhanced as required;
- 8.2.1.4. Managing the full BSC audit by the AGSA from initiation to completion, inclusive of all documentation, meeting minutes etc.

8.2.2. The help-desk manager will be responsible for amongst others the following tasks:

- 8.2.2.1. Defines BIAM system support call management and resolution policies and procedures and oversee the integration with national SASSA help-desk call logging software solution.
- 8.2.2.2. The help-desk defines support tasks, allocates tasks to support staff and monitors BIAM help-desk resources workload and support progress.
- 8.2.2.3. The help-desk manager defines metrics to measure support effectiveness and to assist in measuring resource performance management.
- 8.2.2.4. The help-desk manager is responsible to maintain a consolidated view of service requests across SASSA's Head Office and Regions.
- 8.2.2.5. The help-desk manager monitors the status of service/support calls and oversees the process of service request allocation to SASSA coordinators and system controllers.
- 8.2.2.6. The help-desk manager ensures that support protocol is followed for, service requests, system change requests, configuration baseline requests and releases of approved system changes.
- 8.2.2.7. The help-desk manager ensures that all reports required by SASSA (for monitoring, presentations, reporting etc.) are supplied timeously and correctly.
- 8.2.2.8. The on-going management and reporting of service request will be monitored in weekly and monthly summary that will be conducted by the services and help-desk managers.
- 8.2.2.9. The Agenda for the WEEKLY meetings will cover most of the monthly meeting items in greater detail, as well as the following possible additional items:
 - 8.2.2.10. Help-desk reports
 - 8.2.2.11. Outstanding deliverables
 - 8.2.2.12. Ratio of open to closed calls
 - 8.2.2.13. Categories of calls
 - 8.2.2.14. Severity of calls
 - 8.2.2.15. Action items

8.2.3. The Agenda for the MONTHLY meetings will generally consist of the following items:

- 8.2.3.1. Summary of support calls for the broken down per area and category of call
- 8.2.3.2. Process and technical optimization
- 8.2.3.3. Pressing matters
- 8.2.3.4. Action item reviews
- 8.2.3.5. Future activities
- 8.2.3.6. Prioritizing
- 8.2.3.7. Accomplishments
- 8.2.3.8. Skills and knowledge transfer progress
- 8.2.3.9. Review service levels to date
- 8.2.3.10. Progress against plan – budget (financial control)

The audit and help-desk manager can be combined into a single resource as long as all of the activities are actively and sufficiently dealt with.

8.3. Training Management

8.3.1. The training coordinator will be responsible for, amongst others, the following tasks:

- 8.3.1.1. Create training schedule and publish to Regional Coordinators
- 8.3.1.2. Create catalogue and course content structures on OLM for training and assessments
- 8.3.1.3. Coordinate user access to functions after training has been completed
- 8.3.1.4. Training reports (monthly, quarterly and yearly)
- 8.3.1.5. Identification of training gaps or interventions
- 8.3.1.6. Coordinate training room bookings
- 8.3.1.7. Develop, review and update training materials with UPK
- 8.3.1.8. Provide classroom and online training when required

8.3.1.9. Any other training activities as may be defined from time-to-time

8.4. BIAM Helpdesk Resources

8.4.1. SASSA BIAM system users will report any system queries and/or system problems to the SASSA helpdesk (1st line support) whereby the helpdesk operator will allocate the call to a BIAM Business Support Centre resource.

8.4.2. These calls may also include calls that have been escalated for resolution by SASSA. Each request is termed a Service Request (SR) (not to be confused with the Oracle Service Requests) and will be issued with a service request identifier number.

Logging a service request enables the help-desk to track, categorise and report on the progress of all SR's logged by the SASSA BIAM user community.

8.5. Technical Specialists

8.5.1. The Technical roles consist of the following:

8.5.1.1. System Administrator

8.5.1.2. Oracle DBA

8.5.1.3. Application Server Admin

8.5.1.3.1. Weblogic

8.5.1.3.2. NGINX

8.5.1.3.3. IBM MQ

8.5.1.3.4. BizTalk

8.5.1.3.5. KrakenD

8.5.1.4. Oracle IAM support consultant

8.5.1.5. System Analyst

8.5.1.6. Java Developer

8.5.1.7. Angular Developer

8.5.1.8. Smart Card developer

- 8.5.1.9. BizTalk specialist with development and configuration skills
- 8.5.1.10. Biometric expert to support biometrics best practices with respect to recommending changes/enhancement to SASSA Standard Operating Procedures and processes manual biometrics adjudication guidelines and processes in cases where required (Beneficiary applicants would like a review for rejection due to existing biometrics associated with another beneficiary).
- 8.5.1.11. Neurotechnology specialist with solid SDK and Engine configuration & Administration skills
- 8.5.1.12. IBM MQ specialist with capability to install, configure, and monitor MQ environments. MQ also needs to be upgraded to a later version to enable improved monitoring and operational support.

8.5.2. These roles will be responsible for the administration/ configuration/ maintenance of the respective components:

- 8.5.2.1. Oracle Database (RAC)
- 8.5.2.2. Weblogic servers in a cluster
- 8.5.2.3. Nginx Web servers
- 8.5.2.4. Load Balancers (HAProxy)
- 8.5.2.5. KrakenD – API Gateway
- 8.5.2.6. Custom programs in the environment (NRP, Staff and Beneficiary Enrolment, UI for the fingerprint capture, Software that call the on card API's, Socket Server software, BBE, Card Initialiser software)
- 8.5.2.7. DHA Service Connections: Managing the end-to-end reliability of PIP and PIVA service calls via IJS (BizTalk), direct ABIS/HANIS tunnels, or future-state integration layers.
- 8.5.2.8. IBM MQ for integration with Socpen
- 8.5.2.9. The technical resources must ensure that the components that they responsible for are patched according to the OEM's patch releases to ensure that all security vulnerabilities are mitigated, bugs are fixed and new functionality rolled out.
- 8.5.2.10. These resources are also responsible to monitor the logs of the respective components to identify any errors.
- 8.5.2.11. These resources must also manage the Pre-prod environments.

8.5.2.12. They must assist with DR testing.

8.5.2.13. The DBA's must monitor AWR by running reports from it to identify any performance issues.

9. LOCATION FOR PERFORMANCE OF SERVICES

9.1. On Site Services

9.1.1. SASSA requires that 50% Bidder of the bidder's resources must be on-site in Pretoria and should be competent and capable in the area that they will be supporting the Agency, as well as being fully conversant and fluent in English.

9.1.2. Bidder resources will adhere to all applicable SASSA policies such as the code of conduct, dress code etc.

9.2. Office Accommodation and Other Facilities

To enable the Bidder to provide the Services called for; SASSA will provide, at such time as the Parties shall agree, the following to the Bidder:

9.2.1. Office Accommodation and Related Equipment

9.2.1.1. Office accommodation sufficient to accommodate the Bidder's personnel.

9.2.1.2. The necessary furniture for use by the Bidder's personnel.

9.2.1.3. Where relevant, the necessary network infrastructure, appropriately configured for use by the Bidder's personnel.

9.2.1.4. The successful service provider must provide their resources with laptops that comply with SASSA's security policy.

SASSA can provide the following when the laptops are added to SASSA's domain:

- Anti-virus software and updates on the laptops if required.
- Windows Operating system patching of the laptops if required.
- SASSA will implemented full disk encryption on all laptops used on the SASSA domain

9.2.1.5. Where relevant, access to the necessary server(s), appropriately configured with the required operating system, database and relevant software modules.

9.2.1.6. Telephone and e-mail facilities, provided that these facilities shall be used solely for purposes of the Project.

9.2.1.7. Such other facilities as the Parties may agree from time to time.

9.2.2. Safety

9.2.2.1. Practices as observed by the Basic Conditions of Employment Act will be observed.

9.2.2.2. The Bidder shall ensure that its personnel comply, at all times, with all SASSA safety regulations, such as signing "in and out" every day where applicable.

10. HOURS WORKED AND WORK OUTSIDE NORMAL HOURS

Despite this contract being a full services contract, in other words the Bidder is fully responsible for the provision and successful implementation of all services, SASSA will provide clarity in terms of elements such as office hours and resource numbers and resource levels given the SASSA experience in this regard.

10.1. Normal Working Hours

10.1.1. Maintenance and support should be available from 08:00 to 17:00 Monday to Friday, with a facility for 24x7 support and maintenance outside these hours, as well as over weekends at no additional cost to SASSA.

10.1.2. It should be noted that the DBA usually performs quite a number of their services and functions during the evening.

10.1.3. These timeframes are applicable to all resources.

10.1.4. In the event of a problem which SASSA classifies as critical (e.g. system not functioning), the response time must not exceed 2 hours.

11. RESOURCE REQUIREMENTS: EXPECTED RESOURCES

11.1. SASSA specific Resource Numbers and Levels

- 11.1.1. An experienced Services Manager as specified.
- 11.1.2. A Senior Project Manager to head the Project Management Office,
- 11.1.3. An Audit Manager/Help Desk Manager. One person can also perform the services of the Audit and Help Desk Manager as long as both duties are completed in full.
- 11.1.4. System Administrator
- 11.1.5. Oracle DBA x2
- 11.1.6. Application Server Admin (at least one resource)
 - 11.1.6.1. Weblogic
 - 11.1.6.2. NGINX
 - 11.1.6.3. IBM MQ
 - 11.1.6.4. BizTalk
 - 11.1.6.5. KrakenD – API Gateway
- 11.1.7. Oracle IAM support consultant
- 11.1.8. System Analyst
- 11.1.9. Java Developer x3
- 11.1.10. Angular Developer
- 11.1.11. Smart Card developer
- 11.1.12. BizTalk specialist
- 11.1.13. Biometric expert
- 11.1.14. Neurotechnology specialist with solid SDK and Engine configuration & Administration skills
- 11.1.15. IBM MQ specialist with capability to install, configure, and monitor MQ environments.

11.2. Alignment of Services and Resources

The resource complement prescribed in Section 10.1 has been determined based on the scope, complexity, criticality, and level of services required under this contract. The matrix below illustrates the alignment between the required services and the prescribed resources to ensure adequate capacity and specialist skills for the delivery of the BIAM Support and Maintenance Services.

Required Service	Key Resources Responsible
BIAM application support and maintenance	Services Manager, System Analyst, Java Developers, Angular Developer
Oracle IAM support	Oracle IAM Support Consultant
Database administration	Oracle DBA (2)
WebLogic and middleware support	Application Server Administrator, IBM MQ Specialist, BizTalk Specialist
Help Desk services	Audit Manager / Help Desk Manager, Services Manager
Project management	Senior Project Manager
Audit management	Audit Manager / Help Desk Manager
Fingerprint biometric integration between BIAM and SRD	Java Developers, System Analyst, Biometric Expert, IBM MQ Specialist
Smartcard Initialisation solution	Smart Card Developer, Biometric Expert, Java Developers
Enterprise eKYC implementation	Java Developers, Angular Developer, System Analyst, Biometric Expert, Neurotechnology Specialist
Training and knowledge transfer	Services Manager, Senior Project Manager, relevant Technical Specialists
Disaster recovery support	Oracle DBA, Application Server Administrator, System Administrator
Performance monitoring and tuning	Oracle DBA, Application Server Administrator, Services Manager
24×7 production support (where applicable)	All prescribed technical resources in accordance with their respective responsibilities

The Bidder will be fully responsible and accountable for the management and delivery of services to SASSA and if the service is impacted negatively in any way; SASSA reserves the right to bring on board additional consultants at the expense of the Bidder.

In relation to the aforementioned SASSA requires the CV's of all the recommended resources. Please note that all these resources MUST be available from Commencement Date.

12. CONTRACT AND SERVICE STANDARDS

12.1. Contract

12.1.1. The successful bidder will enter into a contract with SASSA which will outline the overarching timelines and services to be provided under this agreement.

12.2. Measurement of Services and penalties

12.2.1. The Service Level Agreement between SASSA and the Bidder will address the measurement and prioritization of service levels, as well as the response and resolution times.

12.2.2. Penalties associated with the prioritization of service levels and the response and resolution times will be implemented and detailed in the Service Level Agreement.

12.3. Reporting and Communication

12.3.1. The recurring reporting and communication requirements between SASSA and the Bidder will be defined in a Service Level Agreement. It is recommended that communications be open and formal to promote transparency and buy-in (commitment).

12.4. Vetting of all Bidder Resources

12.4.1. Please note that SASSA will request all Bidder resources to undergo a vetting process – given the confidential nature of the SASSA information.

SECTION D – BID REQUIREMENTS

13. SPECIFIC CONTENTS OF THE PROPOSAL

13.1. BID RESPONSE REQUIREMENTS

- 13.1.1. All responses must be prepared as per instructions set out in this bid document. All proposals should be well structured, accurate and unambiguous in their response to the requirements stipulated in the bid document.
- 13.1.2. Bidders must submit a physical document through the SASSA Tender Box at the stipulated address (refer to the advert) and are to submit an electronic duplicate via the e-Tender Portal. The content of both the physical and electronic proposals submitted by the bidders must be the same and any discrepancies will lead to disqualification. No cloud-based links, email submissions or externally hosted documents will be accepted.

The proposal must include as a minimum the following details:

13.2. Previous Experience

1. Oracle IAM Implementation or support&maintenance,
2. Biometric Enrolment (Fingerprint) solution Implementation or support&maintenance ,
3. Biometric Enrolment (Facial) solution Implementation or support&maintenance ,
4. Non-Repudiation Solution using Biometrics Implementation or support&maintenance
5. Biometric deduplication solution Implementation or support&maintenance

13.3. Resources knowledge and experience

- Annexure B must be fully completed:
 - Resources Technical Skills and experience (Please use Annexure B to complete for template
 - The core team and their skills, including their Curricula Vitae should be provided. All resources should be available from Commencement date. A resource's CV used in the bid may be replaced with another resource's that has equal or better knowledge/qualifications and experience.

13.4. Cost Breakdown (Please use Annexure C to complete)

- Please note that the deployment of the eKYC solution will take place on 1 March 2028.

- Accordingly, invoicing for the eKYC implementation may only commence from 1 March 2028.
- Please update and complete the Costing Spreadsheet (Annex C) to reflect these requirements.
- A cost breakdown of the entire support and maintenance service including VAT detailing:
 - Total cost of the all-inclusive BIAM support and maintenance costs:
 - Annually over the 3 year period and
 - on a monthly basis for the duration of the contract.
- Total implementation and support & maintenance cost per sub project:
 - The successful bidder shall modify the BBE application to allow its fingerprint biometric verification and enrolment capability (locally and remotely) to be securely accessed by authorised external systems (including eKYC and OGA).
 - The successful bidder shall design, develop, implement, and maintain a secure smartcard initialisation and personalisation solution. The solution must ensure that each smartcard is uniquely identifiable, securely configured, and cryptographically protected prior to issuance.
 - The successful bidder shall design, implement, and support an enterprise-grade eKYC capability as a shared service. This capability must be consumable through secure APIs by multiple business applications (e.g., SRD, core grants system, and future digital platforms) and must form an integral component of the overall biometric solution. The eKYC capability must also be securely exposed through internet-facing digital channels to enable grant applicants to perform remote identity verification and authentication as part of the application, review, and servicing processes.

NOTE: Bid Evaluation can only be done on the basis of information provided as requested. The comprehensiveness of the bid can therefore be decisive in the awarding of the contract.

13.5. Joint Ventures (JVs)

- 13.5.1. Bidders participating as a Joint Venture (JV), consortium, or similar arrangement shall submit a signed Joint Venture Agreement clearly defining the roles, responsibilities, and obligations of each party.
- 13.5.2. The Joint Venture shall nominate a lead partner who shall be responsible for contract management, communication with SASSA, and overall accountability for the delivery of services under the contract.
- 13.5.3. The combined experience, qualifications, and resources of the Joint Venture partners may be considered collectively for purposes of meeting the minimum requirements specified in this TOR.
- 13.5.4. All resources proposed by the Joint Venture must comply with the requirements set out in Section 10 (Resource Requirements: Expected Resources) and must be available from the Commencement Date.
- 13.5.5. The Joint Venture partners shall be jointly and severally liable for the performance of all contractual obligations arising from this bid.

For purposes of claiming specific goals points,

13.5.5.1. Formal Joint Venture - Incorporated

The Joint Venture or Consortium or Partnership must submit a Joint venture or Consortium B-BBEE Certificate (accredited by the South African National Accreditation System (SANAS) or a sworn affidavit indicating the percentage of all shareholders and signed by Commissioner of oaths, shareholder or owners of company) where applicable. Specific Goals points shall be awarded based on the joint venture or Consortium B-BBEE status level.

13.5.5.2. Informal Joint Venture (Not registered) (Unincorporated)

The Joint Venture or Consortium or Partnership must submit a consolidated B-BBEE Certificate (accredited by the South African National Accreditation System (SANAS) or a sworn affidavit indicating the percentage of all shareholders and signed by Commissioner of oaths, shareholder or owners of company) where applicable. Specific Goals points shall be awarded based on the joint venture or Consortium B-BBEE status level.

13.5.6. Subcontracting and Teaming Agreements.

- Please provide signed agreement.
- Indicate the roles and responsibilities

- Percentage allocation of work

13.5.7. No Consolidated Certificate

If the JV does not submit:

- A consolidated B-BBEE certificate, or
- A valid sworn affidavit (where applicable),

then:

- The bid may still be evaluated, but
- The JV no point will be allocated

SECTION E – EVALUATION INFORMATION

14. EVALUATION OF THE BID

14.0. Bid Evaluation Principles

14.0.1. The bid proposals shall be evaluated in accordance with the 90/10 principle. The evaluation shall be conducted as follows:

i. First Stage;

- Phase 1 : Special Condition
- Phase 2; Administrative Compliance;
- Phase 3; Functionality Criteria;

ii. Second Stage – Price and Preference Points.

14.0.2. Responses to the functional requirements must be attached as directed, using the response template provided.

Phase One – Special condition

Oracle Partnership Certification

The bidder shall provide proof of its current Oracle partnership status by submitting either of the following:

- A valid Oracle Partner Certificate; or
- An official letter from Oracle (OEM) confirming the bidder's current Oracle partnership status.

Please note that SASSA will verify the authenticity, validity and status

(good standing) of the submitted certificate or letter directly with Oracle.

Note: Failure to submit either a valid Oracle Partner Certificate or an official letter from Oracle confirming the bidder's partnership status will invalidate your bid.

Phase Two - Administrative Compliance

Bidders should submit the following:

- Tax Status Verification Pin
- Central Supplier Database (CSD) report
- B-BBEE Certificate issued by SANAS / Sworn Affidavit to claim points in line with the below Special Goals
- SBD Forms

NOTE: Failure to submit the above may invalidate your bid.

Phase Three: Functionality Criteria

14.0.3. The table below contains details of the evaluation criterion and the weights of each Functional Requirements component.

14.0.4. Criteria below will be evaluated according to the following values

1=Poor 2=Average 3=Good 4=Very Good 5=Excellent

Phase 3: Functionality Criteria

EVALUATION CRITERIA	
Phase Two – Functionality Criteria	Weights
Required Experience : Bidders are required to fully complete spreadsheet Annexure A	
○ Oracle IAM Implementation\Support & Maintenance projects	10
○ Biometric Enrolment (Finger) Implementation \Support & Maintenance Projects	10

○ Biometric Enrolment (Facial) solution Implementation or support&maintenance	15
○ Non-Repudiation Solution using Biometrics Implementation\Support&Maintenance Projects	15
○ Biometric deduplication solution Implementation\Support&Maintenance Projects Each of the required experiences listed above will be scored as follows: Less than 1 year of implementation/support experience = 1 At least 1 year but less than 2 years of implementation/support experience = 2 At least 2 years but less than 3 years of implementation/support experience = 3 At least 3 years but less than 4 years of implementation/support experience = 4 5 years or more of implementation/support experience = 5 SASSA will verify information provided in Annexure A, as well due diligence, therefore it's the bidders responsibility to supply verifiable information Successfully verified references will be allocated appropriate score. Resources • Comprehensive CV(s) highlighting relevant experience and skills as per above paragraph 10 of Resource Requirements: Expected Resources Less than 2 year of experience = 1 At least 2 year but less than 5 years of experience = 2 At least 5 years but less than 8 years of experience = 3 At least 8 years but less than 10 years of experience = 4	40

10 years and above experience = 5	
TOTAL	100

NB. Bidders who score less than **70 of the 100** points of the Functionality Points will be disqualified, and thus will not be evaluated further.

SECOND STAGE: PRICE AND PREFERENCE POINTS (SPECIFIC GOALS)

Points awarded for price and specific goals

Price and Preference point system	100
Price	90
Specific Goals	10

Price

$$P_s = 90 \left(1 - \frac{P_t - P_{min}}{P_{min}} \right)$$

Where

P_s = Points scored for price of tender under consideration

P_t = Price of tender under consideration

P_{min} = Price of lowest acceptable tender

Preference Point (Specific Goals)

Specific Goals	Number of points (90/10 system)
B-BBEE Status Level 1-2 contributor with at least 51% black women ownership	10

B-BBEE Status Level 3-4 contributor with at least 51% women ownership	9
B-BBEE Status Level 1-2 contributor with at least 51% youth or disabled ownership	8
B-BBEE Status Level 1-2 contributor	7
B-BBEE Status Level 3-8 contributor with at least 51% youth or disabled ownership	5
B-BBEE Status Level 3-4 contributor	3
B-BBEE Status Level 5-8 contributor	2
Others	0

1.3.1. Bidders to submit a B-BBEE verification certificate from a verification agency accredited by the South African National Accreditation System (SANAS) or a sworn affidavit indicating the percentage of all shareholders and signed by Commissioner of oaths, shareholder or owners of company.

1.3.2. Failure to submit shall be interpreted to mean that preference points for B-BBEE status level of contribution are not claimed.

Note: A tenderer must submit proof of its B-BBEE status or supporting documents for the above listed specific goals

15. QUESTIONS AND ANSWERS TO THIS BID

All enquiries, questions and requests for clarification that may arise in relation to this Bid is to be done in writing and addressed to the below email address listed in the Invitation to Bid.

biamsrd2021@sassa.gov.za

It is important to note that for all with questions to be clearly and precise.

The emails also include:

- Bid Ref# in the subject line of your e-mail as per the advert
- Company's name,
- The company representative
- Contactable number (telephone number and/or Cell phone number)
- Submitting of questions on the date of closure will not result in the extension of the Bid closing date and time

Bidder to send question/s within 5 days of the advert and SASSA will respond with 7 days of the bid advert.

Question and Answers will therefore be uploaded on SASSA website

<https://www.sassa.gov.za/>

16. BID CONDITIONS

- 16.1. SASSA reserve the right to negotiate price with the preferred bidder. Price negotiation will follow the guidelines as stipulated under the Heading “10. Negotiations with Bidders” of the Supply Chain Management Preferential Procurement Policy, signed on the 15 January 2023.
- 16.2. Bidders should ensure that resources provided in this bid and after award are fluent in English both verbally and written.
- 16.3. It's the bidder's responsibility to submit valid evidence such as B-BBEE verification certificate issued by South African National Accreditation System (SANAS) and/or a sworn affidavit signed by Commissioner of oaths, shareholder or owners of company) and/or CSD MAAA Number reflecting the percentage of the company ownership including B-BBEE status level of contribution to enable claiming of point for Special Goals. A sworn affidavit must be submitted over and above the B-BBEE certificate or CSD MAAA Number to claim for the below contributor level:
- B-BBEE Status Level 1-2 contributor with at least 51% youth or disabled ownership
 - B-BBEE Status Level 3-8 contributor with at least 51% youth or disabled ownership
- 16.4. SASSA reserves the right to perform due diligence related to any information provided by the bidder and any misrepresentation of the information may lead to disqualification of your proposal or termination of the contract.
- 16.4.1. Failure to submit evidence to claim special goals shall be interpreted to mean that no points are claimed.
- 16.5. Bids must be submitted in line with any attached annexures, detailed specifications.
- 16.6. The Agency reserves the right to award the bid: - or not to award the bid at all.

- 16.7. The Agency will contract and also conclude Service Level Agreement(s) with the successful bidder.
- 16.8. The General Conditions as stipulated by the National Treasury will be applicable.
- 16.9. Bid rigging (or collusive bidding) is prohibited and this occurs when businesses, that would otherwise be expected to compete, secretly conspire to raise prices or lower the quality of goods and / or services for purchasers who wish to acquire goods and / or services through a bidding process. Bid rigging is, therefore, an agreement between competitors not to compete.