

DRIVING NEW FRONTIERS FOR SUSTAINABLE GROWTH

Request for Proposal for Acquisition of Application Programming Interface (API) Management Solution for a Period of 60 months at Airports Company South Africa.



**AIRPORTS COMPANY
SOUTH AFRICA**

AGENDA

- 
- 1 Introductions
 - 2 Bid Schedule
 - 3 General Administration
 - 4 Minimum Administrative Requirements
 - 5 Evaluation Criteria
 - 6 Tender Document Organisation
 - 7 Bidders Response File
 - 8 Technical Requirements
 - 9 Questions
 - 10 Closing Remarks



AIRPORTS COMPANY
SOUTH AFRICA





BID SCHEDULE

| Activity | Date |
|-----------------------------|---------------------------|
| Bid Advertisement | 28 February 2023 |
| Bid documents issued | 28 February 2023 |
| Optional Briefing Session | 10h00, 10 March 2023 |
| Enquiries and clarification | 24 March 2023 at 17h00 PM |
| Tender Closing date | 12h00, 31 March 2023 |
| Bid Evaluation | April 2023 |
| BAC Submission | April 2023 |
| Award to Successful Bidder | May 2023 |





GENERAL ADMINISTRATION

- **ENQUIRIES AND CLARIFICATION:**

- To be directed to sydney.mfeka@airports.co.za cell : 062 934 0554
- **All enquiries must have a tender reference number and description on the subject of the email**

Please submit your submission through email to **Sydney.Mfeka@airports.co.za**. On the subject of the email use the following **“COR7057/2022/RFP”- Request for Proposal for Acquisition of Application Programming Interface (API) Management Solution for a Period of 60 months at Airports Company South Africa.**

- RFP Submission checklist in conjunction with Functional/Technical evaluation criteria elements
- **SUBMISSION AND CLOSE OF BID: Friday, 31 March 2023 and closes at 12:00pm**
- **Please note: No bid shall be accepted after the closing time**



EVALUATION PROCESS

| Stage 1 | Stage 2 | Stage 3 | Stage 4 | Stage 5 | Stage 6 |
|--|------------------------|---|--------------------------------|---------------------------|------------------|
| Check if all the documents have been received. | Mandatory Requirements | Evaluate on functionality or the technical aspect of the bid. | Evaluate price and Preference. | Post tender negotiations. | Security Vetting |



MANDATORY REQUIREMENTS

- Bidders must provide the certification for the cloud environments being utilized as being certified in the ISO/IEC 27001.
- Bidders must provide a plan of how they will secure ACSA's data.
- Company, its directors and employees agree to be vetted by Airports Company South Africa (ACSA).



MINIMUM ADMINISTRATIVE REQUIREMENTS

** ACSA will only award this tender to a bidder whose tax affairs have been confirmed to be in order. Provide the valid pin.

Bidders must be registered on Central Supplier Database (CSD), Attach CSD registration Certificate.

Bidders MUST meet the Minimum Administrative Requirements.

Compliant (Compliant) bids will then proceed to next phase of evaluation



EVALUATION CRITERIA

Hurdle phase - Bids MUST obtain Minimum qualifying score of 70 points in order to proceed to the next phase of the evaluation. **Annexure A and B is very critical.**

DEMONSTRATE THE EVALUATION CRITERIA



TENDER DOCUMENT ORGANISATION

The Tender Pack is organised as follows

- **RFP Document**
 - Annexure A - Scope of work
 - Annexure B – Evaluation Criteria
 - Annexure C - Pricing Schedule
 - Annexure D – IT Service Management Roles and Responsibilities
 - Annexure E – Insurance Requirements.



NOTICE

Bidders are requested to always check on e-tenders portal for the updates.

All Questions and Answers will be posted on e-tenders portal

www.etenders.gov.za

And any other updates



BIDDERS RESPONSE FILE

Bidders are required to ensure that each returnable document is returned under the correct Appendices as shown in the Main RFP document.





TECHNICAL

ACSA requires an API Management solution that will enforce ACSA's policies, control access, collect and analyze usage statistics and report on performance. The solution must also integrate with the existing solutions specified above. The solution must have the following core components:

- ❑ **API Gateway:** a server that acts as an API front-end, receives API requests, enforces throttling and security policies, passes requests to the back-end service and then passes the response back to the requester.
- ❑ **API Lifecycle Management:** ability to define or publish APIs.
- ❑ **API Developer portal:** community site that is a source of information (including documentation, tutorials, sample code, software development kits, an interactive API console and sandbox to trial APIs and obtain support from the API provider and user community).
- ❑ **API Analytics:** functionality to monitor API usage as well as diagnostics.



TECHNICAL

➤ API Management Solution Key Features & Capabilities

- ❑ Support different third-party connectors and adaptors to a wide variety of applications, either hosted On-Premises or Cloud.
- ❑ Faster development of complex integration flows and scenarios using pre-built connectors/integration templates, i.e., to improve time to market.
- ❑ Enable data transformation and transmission effortlessly, e.g., CSV, XML, JSON, Low-code, etc.
- ❑ Support for real-time and batch integration.
- ❑ Security features such as access management, LDAP integration and encryption.
- ❑ Centralized platform for administration and monitoring, e.g., resource utilisation and system health.



TECHNICAL

- ❑ Ability to provision, manage and monitor APIs, i.e., API Management.
- ❑ Keep APIs up to date with API changes and services.
- ❑ Ability to manage API to discover all available services.
- ❑ Control and manage API access authentication.
- ❑ Scalable to be able to manage additional traffic and requests.



TECHNICAL

➤ API Management Solution must be able to do the following :

- ❑ API management supports APIs' planning, design, implementation, publication, operation, versioning, and retirement. API management implements key governance features and manages access to any endpoint that exposes an API (i.e., whether On-Premises, in the Cloud, Mobile or IoT).

➤ API Lifecycle Management

- ❑ The solution must support the entire lifecycle of API delivery (build, deploy and manage) for both On-Premises and Cloud applications.
- ❑ The solution must be able to provide APIs for internal and external consumption.
- ❑ The solution must be able to set up and administer integrations using a user-friendly interface that requires low coding.

➤ Communication Protocol Connectors

- ❑ The solution must be able to interact with applications and data structures using different protocols (such as HTTP, HTTPS, FTP, TCP/IP, AMPQ, JMS, ODBC, etc.).





TECHNICAL

➤ Application and Data Connectors

- ❑ The solution must be able to establish connectivity to different applications and data sources via a variety of adapters and interfaces. The following are critical applications used at ACSA: Airport Management Suite (On-Premises), Apex (On-Premises), Oracle E-Business Suite (On-Premises), Oracle Taleo (Cloud), Oracle Fusion (Cloud), Oracle Learn (Cloud), ServiceNow (Cloud), Microsoft SharePoint (On-Premises), Active Directory (Cloud), E-Gates, SAC, SCORE, 2D Barcode, BRS, ACSA website (Flight Information), Aircraft Docking System, Oracle ERP (Billing Data), Ground Radar (ATNS), Retail and many more.

➤ File Transfer/Movement

- ❑ The solution must be able to distribute files between systems on a automated and scheduled or manual basis, e.g., FTP directory or HTTP URL.
- ❑ The solution must have a retry mechanism where it can send unsuccessful request.

➤ Messaging

- ❑ The solution must be able to distribute messages between endpoints. The messaging broker platform must enable publish-subscribe, message queueing or both.



TECHNICAL

➤ Protocol Mapping

- ❑ The solution must be able to map between different endpoint protocols, such as a file to a message, application connector to the data source or any combination of points.

➤ Data Formats

- ❑ The solution must be able to process different data formats such as XML, JSON, and flat files, etc. and much more.

➤ Routing and Orchestration

- ❑ The solution must be able to route data between endpoints and orchestrate the flow of information across those endpoints.

➤ Data Mapping and Transformation

- ❑ The solution must be able to map, transform, aggregate and split data between different data formats and industry standards.
- ❑ The solution must provide standard tools and functions to convert data values from a source system's data format into a destination system's data format.

➤ Data Lifecycle Management

- ❑ The solution must manage data flow throughout its lifecycle: from creation and initial storage to obsolescence and deletion



TECHNICAL

➤ Master Data Management

- ❑ The solution must support managing master data by removing duplicates and using rules to eliminate incorrect data from entering the system.

➤ Data Standards

- ❑ The solution must integrate different data sources (Oracle, MS SQL, Hadoop, DB2, PostgreSQL, etc.) using industry standards, e.g., data structure, data content, data value, and data communication. The solution must be data-agnostic, i.e., manage Structured, semi-structured, and unstructured data.
- ❑ The solution must integrate into different Businesses using Open and Industry Standards enabled; ACI ACRIS and IATA AIDX compatible.

➤ Data Integration

- ❑ The solution must integrate with both On-Premises and Cloud data sources.
- ❑ The solution must be able to schedule jobs based on defined rules or processes.
- ❑ The solution must be able to manage streaming, real-time, event-driven, and batch data.
- ❑ The solution must change with the evolving data sources landscape and be able to manage new data source standards introduced in the IT industry, e.g., Cassandra, HBase, Neo4j, Arango, Mongo and etc.
- ❑ The solution must support bi-directional data synchronization between ACSA and 3rd parties.



TECHNICAL

➤ API Standards

- ❑ The solution must support multiple open and modern API standards such as JMS, MQI and Web Services (SOAP & REST) models, etc.

➤ Integration

- ❑ The solution must seamlessly integrate with Enterprise Service Bus , Message Queue , Message Broker , DataPower Appliance and MQ Appliances
- ❑ Oracle Database
- ❑ SQL Database

➤ Reusable APIs

- ❑ The solution must be able to discover existing API integrations for reuse.
- ❑ The solution must have the ability to reuse schemas and data models.

➤ Testing

- ❑ The solution must be able to test integrations before deploying them to a production environment, i.e., without interfering with the live production systems.



TECHNICAL

➤ Version Control

- ❑ The solution must have version control capabilities to enable roll-back when APIs are incorrectly provisioned.
- ❑ The solution must be able to record version history.

➤ API Monitoring

- ❑ The solution must manage and monitor created APIs to ensure they work as intended.
- ❑ The solution must notify the relevant stakeholders if there are issues with the created APIs, e.g., the API is down due to network problems.

➤ API Collaboration and Community

- ❑ The solution must have a community forum containing an API provider blog, Developer discussion forums, and Developer issue reporting.

➤ Monetization

- ❑ The solution must assist ACSA in collecting revenue based on API usage, i.e., have the ability to bill stakeholders based on API usage.
- ❑ The solution must be able to set up pricing rules based on usage, load and functionality.

➤ Emerging Technologies

- ❑ The solution must integrate emerging technologies as well as evolve and manage new API standards introduced in the IT industry, e.g., Swagger 2.0 and GraphQL, etc.



TECHNICAL

➤ Reporting and Analytics

- ❑ The solution must provide an integration landscape (including data source integrations and services offered), i.e., API Catalog.
- ❑ The solution must also have a graphical representation of data structures (including data fields that have been mapped).
- ❑ The solution must be able to provide statistics on the utilisation of APIs.



The solution must report on top applications using API's.

- ❑ The solution must provide a Centralised monitoring dashboard for all integration flows in real-time.
- ❑ The solution must report on system health, such as any issues that exist in the environment.
- ❑ The solution must provide insights into performance and capacity.
- ❑ The solution must allow ACSA to customise its reports.
- ❑ The solution must report on security compliance and any other vulnerabilities that must be addressed.



TECHNICAL

Non-Functional Requirements

➤ Hosting

- ❑ The solution must be hosted in a Tier 2 level or more data center, i.e., Cloud-based.
- ❑ Regulatory and compliance certificates must be provided an ISO/IEC 27001 certificate.
- ❑ The platform must be a standalone service and not an embedded subset of another SaaS application.

➤ Platform performance (Speed & Latency)

- ❑ The solution must respond quickly when users are working on it, i.e., not click a section and wait for more than 5 seconds.
- ❑ The solution must be able to manage volumes during peak times.
- ❑ The solution must cater for bandwidth constraints and geographically dispersed systems.

➤ Scalability

- ❑ The solution must cater for future growth, e.g., adding new APIs, Connectors, i.e., no limitation to the number of APIs that can be added.
- ❑ The solution must be able to expand functionality while maintaining balanced loads. It must also have the ability to serve growing demand without reducing functionality.

➤ Usability

- ❑ The solution must be easy to use with minimal user training, i.e., Web-based



TECHNICAL



➤ Reliability & Availability

- ❑ The solution must be available 24/7 with a minimum availability of 99.8%.
- ❑ The solution must cater for high availability.
- ❑ The solution must be backed up daily and have offsite backup storage.
- ❑ The solution must allow users to recover deleted data by requesting a restore or independently recovering the deleted data.

➤ Security

- ❑ The Service Provider must provide ACSA with their security best practices or controls detailing how they secure their solution.
- ❑ The solution must ensure that data is transmitted in a non-readable format (encrypted) and has strong key management. The solution must provide encryption capabilities for stored data to ensure that data at rest is protected.
- ❑ The Service Provider must ensure that Server-level security features are in place for the solution. They must provide information related to the following: patching, anti-virus, vulnerability scanning, intrusion detection with real-time alerts etc.



TECHNICAL

- ❑ The Service Provider must ensure that Data Center security features are in place. They must provide information related to the following: Physical security measures, which include an integrated security management solution such as around-the-clock on-site security personnel, video surveillance, and monitoring—as well as industry-leading policies and practices.
- ❑ The solution must also detect anomalies in functionality, user accessibility, traffic flows, and tampering.

➤ Authentication

- ❑ The solution must uniquely identify users and authenticate them. Administrator accounts must be segregated from standard user accounts.

➤ Authorization

- ❑ The solution must enable users and/or role-based permissions to be configured to control what solution features and data users can access.



TECHNICAL

➤ Audit Trail

- ❑ The solution must keep an audit trail of all activities performed in the solution (includes but is not limited to the following: who created, updated, and deleted (must be authorised by super users) the record, with time and date stamp.

➤ Assurance

- ❑ The solution must maintain data integrity and quality. The solution must be a single source of truth in terms of data and quality.

➤ Availability

- ❑ The solution must be secured to prevent denial of service to ACSA users. It must also provide threat protection

➤ Asset Protection

- ❑ The solution must protect ACSA data from being viewed by unauthorised personnel.
- ❑ The solution must limit access to suspicious visitors and monitor for traffic spikes to prevent overloads like DDoS attacks.



TECHNICAL

➤ Privacy and data ownership

- ❑ The solution must comply with ACSA's Information Security policies and standards (to be provided to the Service Provider once the contract agreement is awarded).
- ❑ The solution must comply with POPI Act and other related laws or regulations. All data remain the property of ACSA.
- ❑ The Service Provider must detail their conformity to data / Information Security Management / ISO/IEC 27001.

➤ Solution Accessibility

- ❑ The solution must be accessible in one central platform, i.e., ACSA must only use one interface instead of multiple products.
- ❑ The solution must be accessible via laptops, desktops, and mobile devices.

➤ Disaster Recovery

- ❑ The solution must have an alternative way to ensure business continuity in cases with an unfortunate downtime event.
- ❑ The solution disaster recovery must be tested at least once annually and also be audited by an external audit company



TECHNICAL



➤ Local Support

- ❑ The solution's first-line support solution must be based in South Africa (international support can form part of the 2nd and 3rd line support).

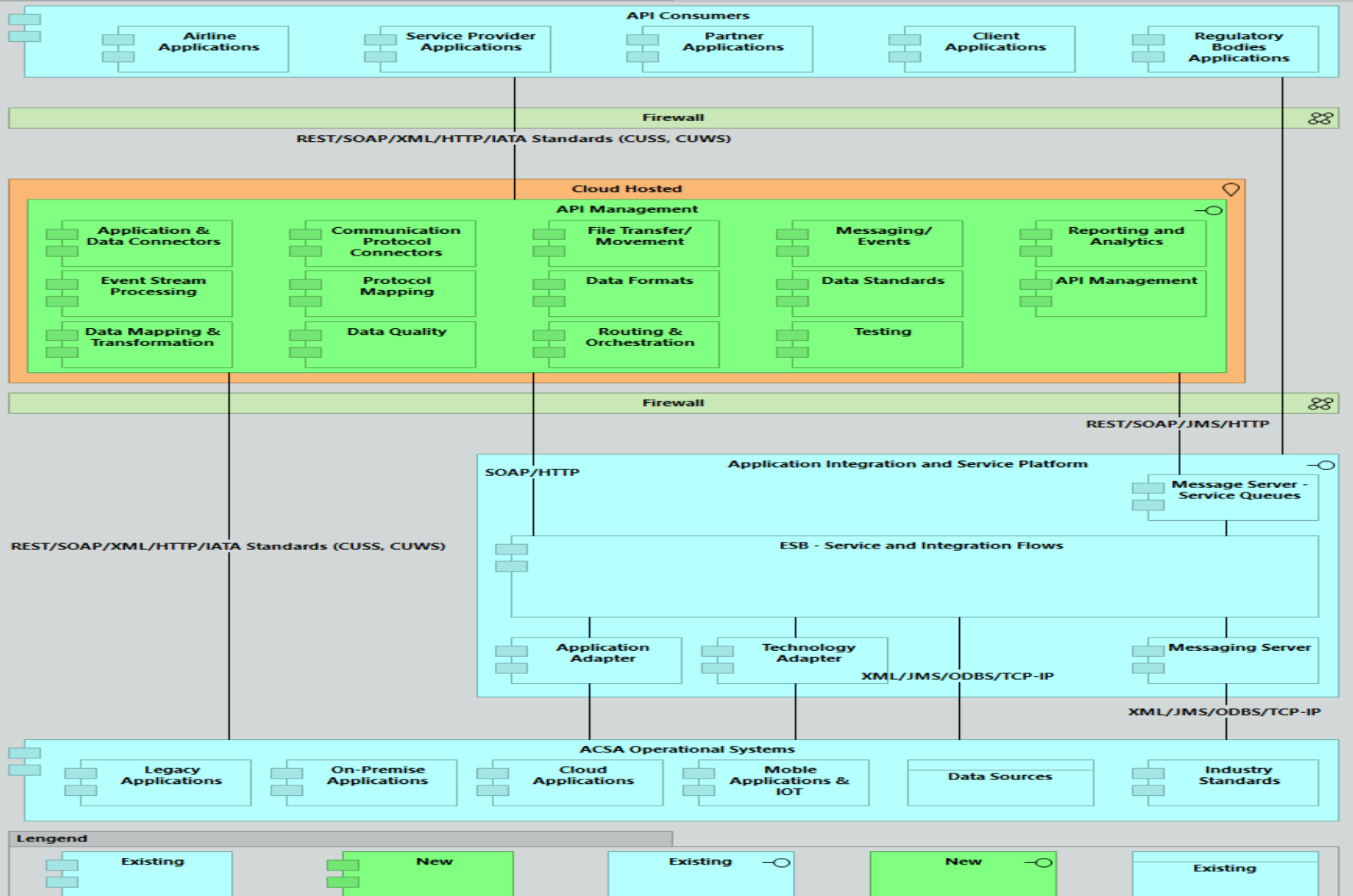
➤ Environments (Development, Quality Assurance and Production)

- ❑ Multiple environments, i.e., Production and non-production environments. The solution must be able to migrate a customised development environment to a quality and production environment.



TECHNICAL

API Management





QUESTIONS





CLOSING REMARKS

- FEEDBACK ON ACSA TENDER PROCESS; AND
- ERRORS IN THE TENDER DOCUMENT
- ACSA CONTRACT TEMPLATE TO BE USED – PROPOSED AMENDMENTS



**THANK YOU
&
GOOD LUCK!**

