Annexure A

Electronic Signature Solution

Scope of Work


**Glossary**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACSA</td>
<td>Airports Company South Africa</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>SOC</td>
<td>State owned Company</td>
</tr>
</tbody>
</table>

**Version history**

<table>
<thead>
<tr>
<th>Version#</th>
<th>Author</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Sharon Makgato</td>
<td>Signed-off</td>
</tr>
<tr>
<td>1.1</td>
<td>Rets’elisitsoe ‘Molaoa</td>
<td>Effected updates received from reviewers.</td>
</tr>
<tr>
<td>1.2</td>
<td>Rets’elisitsoe ‘Molaoa</td>
<td>Effected updates as per TPEC</td>
</tr>
<tr>
<td>1.3</td>
<td>Rets’elisitsoe ‘Molaoa</td>
<td>Effected updates as per tender feedback</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1. Introduction
   1.1 Purpose
   1.2 Objective
   1.3 Background
   1.4 RFP Scope
   1.5 ACSA Business Requirements
   1.6 Integration Requirements
   1.7 Security Requirements
   1.8 Legislature Requirements
   1.9 Required Services from the Bidder
2. Support
3. Reporting
4. Documentation
5. Pricing schedule
6. Maintenance and Support
   Evaluation Criteria
   Approvals

Scope of work document for the eSignature Solution
1. Introduction

1.1 Purpose

The purpose of this document is to detail business and systems requirements which will be used by SCM to go out to market to invite suppliers to bid in providing the desired solution as outlined in the requirements specified in this document.

1.2 Objective

It is required that a Service Provider be appointed to supply; implement; support and maintain a digital signature solution to enable the reviewing, tracking and signing of electronic documents. The solution will enable online signing and reduce the need for physical sign-off of documents. This is particularly important for Executives, Group Managers, Senior Managers, Managers and Supervisors who are not always physically present to sign-off documents. The solution will aid efficiency as approvals can be done remotely via this digital signature solution. It will further limit the use of paper and is a key step on the journey to a paperless and digitized ACSA. This will improve the approval process by eliminating the need to print, sign and scan documents. It will further improve the tracking process and audit trails. The service provider is required to supply the digital software, implement it, host the service; and provide maintenance and support for the period of five years.

1.3 Background

ACSA has implemented the Microsoft SharePoint technology to facilitate the management of documents and records and further allow for the introduction of workflow. There is a need to improve on electronic document processes by introducing the concept of signing documents digitally.

1.4 RFP Scope

1.4.2. The scope of the solution will cover the Corporate office and 9 Airports sites; OR Tambo, Cape Town, King Shaka, Braamfischer, Upington, Kimberley, George, Port Elizabeth and East London.

1.4.3. Estimated number of users is 750, categorized into advanced digital signature (token or other multifactor authentication) and regular users.

1.4.3.1. Advanced digital signature users – estimated to be +/- 130
1.5 **ACSA Business Requirements**

1.5.1. Solution should be able to provide digital signature capability for the documents within SharePoint and as a stand-alone (on laptops etc).

1.5.2. The solution should provide functionality to sign documents digitally and easily send documents for digital signature. This includes the ability to provide real-time visibility into the status of a document.

1.5.3. It should provide the ability for real-time visibility of the status the document sign-off request is in. This will enable the user requesting sign-off to know when the document is opened; signed; or returned.

1.5.4. It should provide functionality to add the names, SharePoint groups (integrate with AD) and email addresses of the individuals (recipients) who needs to sign the document and provide an option to specify the order of signing and re-assignment option.

1.5.5. The solution must be able to add signature blocks to all documents formats and automatically convert to PDF for signature.

1.5.6. The solution should provide sufficient security and advanced authentication methods (2 factor authentication) to validate the signatory’s identity and the data should be securely encrypted.

1.5.7. An audit trail of the document workflow information should be retained for proof of compliance, from initiation to completion.

1.5.8. A workflow process which will record an audit trail including the status of a user’s document that indicates when the document was uploaded, sent, who it was sent to, when was it opened, signed, and returned.

1.5.9. The resulting digital signatures should be legally enforceable (digital signature evidence should be admissible in a court of law).

1.5.10. The solution should also work on mobile devices e.g. smartphone (Android and iOS) and tablets. This will enable users to review and sign documents using mobile devices.

1.5.11. The resulting digital signatures should be legally enforceable ensuring non-repudiation.

1.5.12. The system should be able to detect changes in the document and invalidate all signature already on the document.

1.5.13. The documents put through the digital signature solution workflow must always be secured. They must only viewable by parties who are meant to view them.

1.5.14. With the implementation of the digital signature solution, ACSA’s data classification policy must be taken into account (to be provided to the winning bidder)
1.6 Integration Requirements
The solution should be able to integrate with SharePoint 2013. It should be able to send the document link (one document to multiple recipients) via email to the individuals (recipients) who need to sign. Once the document is complete and signed, it should be stored securely for easy retrieval.

1.7 Security Requirements
The Service Provider will be expected to comply with ACSA networks and information security standards. ACSA reserves the right to audit the environment where the solution will be hosted the cost of which will be incurred by ACSA.

1.8 Legislature Requirements
The Service Provider should be compliant with Protection of Personal Information Act (POPIA) to ensure that ACSA employees' personal details in their possession is protected.

1.9 Required Services from the Bidder
1.9.1. Host the solution for the period of 5 years
1.9.2. Face to face verification, registration and enrolment for all in scope users
1.9.3. Supply digital signature certificates for all the users
1.9.4. Enrolment, verification and Training of ACSA digital signature Administrator
1.9.5. Configuration of end user devices, i.e. Laptops, tablets and smartphones
1.9.6. Training of the users at corporate and all in scope ACSA sites. This is not a train the trainer approach but rather training of all users.

2. Support
Support services refers to day to day support activities performed to resolve incidents that are logged by users of the system or logged by the monitoring tools or alarm and error logs generated by the system’s internal monitoring. The Service Provider will be expected to provide technical support to manage the solution for a period of five years. The support will cover upgrades and patches and updates of the digital signature software. Below are the service requirements:

2.1 The Service Provider will be required to attend to and resolve all incidents in line with ACSA incident management processes;
2.2 All incidents will be logged on the IT service desk systems. The response and resolution times depicted in times must be adhered to;
2.3 This will form part of the SLAs that will be agreed to between the Service Provider and ACSA; and

2.4 Penalties will be incurred by the Service Provider if the agreed SLA times are not met.

2.5 Incident logging procedure

   a) All incidents must be logged with ACSA service desk via email or telephone
   b) The incident status must be updated regularly depending on the priority of the incidents until resolution; and
   c) All incidents must be updated with a detailed resolution before closure. The Service Provider must notify the service desk immediately on resolution of the incident.

Definition of incident priority

<table>
<thead>
<tr>
<th>Item #</th>
<th>Priority</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>P1</td>
<td>Total systems failure/server down or complete loss of system functionality in one or more areas of the airport. The failure has a negative impact to the airport’s operation.</td>
<td>Critical</td>
</tr>
<tr>
<td>2.</td>
<td>P2</td>
<td>Multiple devices are down simultaneously however with minimum functionality in the area.</td>
<td>High</td>
</tr>
<tr>
<td>3.</td>
<td>P3</td>
<td>Failure of single device or components of the systems.</td>
<td>Medium</td>
</tr>
<tr>
<td>4.</td>
<td>P4</td>
<td>Non-critical fault/failure logged at night or over the weekend. It has no impact on the operations of the airport.</td>
<td>Low</td>
</tr>
</tbody>
</table>

Table 1: Incident Priority Definitions

Applicable incident management response as well as resolution times are articulated in below:

<table>
<thead>
<tr>
<th>Incident Priority</th>
<th>Response</th>
<th>Restoration</th>
<th>Update Feedback</th>
<th>Resolution (permanent fix)</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>15min</td>
<td>2hrs</td>
<td>15min</td>
<td>Within 6 hours</td>
</tr>
<tr>
<td>P2</td>
<td>30min</td>
<td>4hrs</td>
<td>30min</td>
<td>Within 12 hours</td>
</tr>
<tr>
<td>P3</td>
<td>60min</td>
<td>4hrs</td>
<td>2hrs</td>
<td>Within 24 hours</td>
</tr>
<tr>
<td>P4</td>
<td>4hours</td>
<td>24hrs</td>
<td>6hrs</td>
<td>Within 48 hours</td>
</tr>
</tbody>
</table>

Table 2: Incident Response and Resolution Times
2.6 Availability requirements

An ACSA availability requirement for digital Signature is 99.9% per month. The Service Provider must ensure that the availability targets are met every month. In an event that the target is not met ACSA will impose penalties. The formula for calculation will be provided to the successful Bidder.

The digital signature service should be available 24/7 and should allow employees to sign remotely when connected to the ACSA domain on site or via VPN.
2.7 Penalties

The following penalties shall apply for failure to resolve incident within the agreed timeline:

<table>
<thead>
<tr>
<th>Item #</th>
<th>SLA breach</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>P1 Incidents are resolved within one hour after SLA time lapsed for two</td>
<td>20% of the monthly fee will be deducted per invoice up to 60% in one contractual year thereafter termination procedures will be implemented.</td>
</tr>
<tr>
<td></td>
<td>consecutive times in a measuring period.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Incidents are resolved within two hours and beyond after SLA time lapsed</td>
<td>30% of the monthly fee will be deducted up to 60% in one contractual year thereafter termination procedures will be implemented.</td>
</tr>
<tr>
<td></td>
<td>for three consecutive times.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>If a Service Provider misses SLA’s in any 3 consecutive months.</td>
<td>50% of the monthly fee will be deducted.</td>
</tr>
<tr>
<td>4.</td>
<td>Fourth missed SLA in one month— will be deemed as a material breach, and</td>
<td>50% of the monthly fee will be deducted.</td>
</tr>
<tr>
<td></td>
<td>the contract will be referred for performance management and termination</td>
<td></td>
</tr>
<tr>
<td></td>
<td>procedures.</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: SLA Breach and Penalty Rates

Failure to perform preventative maintenance according to schedule dates shall result in the following penalties

<table>
<thead>
<tr>
<th>SLA breach</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance not done or proof not submitted.</td>
<td>No payment</td>
</tr>
</tbody>
</table>

3. Reporting

The Service Provider will be expected to provide the progress reports to an ACSA representative weekly during implementation.

Once the implementation has been implemented the Service Provider is to provide monthly reports to ACSA on the following

- Usage in terms of number of signatures
- Service availability (if any)
- Number of calls logged and status.
4. **Documentation**

The following project related documentation must be produced by the Service Provider on completion of the project:

- Functional Specification
- Technical Specification
- Test results
- Training Manuals
- Additional documents may be required once the solution is in production i.e. system performance reports; issue log sheets etc.

5. **Pricing schedule**

The bidder must clearly indicate the cost separately for the following:

6.1 Software
6.2. Solution Configuration and implementation
6.3. Hosting
6.4. Enrolment of users
6.5. Training
   6.5.1. Technical resources
   6.5.2. Service Desk
   6.5.3. End Users

6. **Maintenance and Support**

Bidders are expected to provide a pricing schedule for both preventive and corrective Maintenance as well as support. The schedule should include but not limited to the following:

- Maintenance type
- Frequency
- Period (i.e. during the week, weekend and public holidays)
- Cost
- Resource title