EXPRESSION OF INTEREST FOR THE PROVISION OF AUDIT SERVICES FOR SECURE ELECTRONIC SIGNATURE PROVIDERS FOR

BOTSWANA COMMUNICATIONS REGULATORY AUTHORITY

REFERENCE NO. BOCRA/PT/008/2017.18

Tender Closing Date 8th December 2017
SECTION 1 Terms of Reference

TERMS OF REFERENCE

FOR THE

PROVISION OF AUDIT SERVICES FOR SECURE ELECTRONIC SIGNATURE

PROVIDERS TO

BOTSWANA COMMUNICATIONS REGULATORY AUTHORITY
1. BACKGROUND, PURPOSE AND SCOPE OF SERVICES

1.1 Introduction

Botswana Communications Regulatory Authority (BOCRA or the Authority) was established through the Communications Regulatory Authority Act, 2012 (CRA Act) on the 1st of April 2013 to regulate the communications sector in Botswana, comprising telecommunication, Internet and Information and Communications Technologies (ICTs), radio communications, broadcasting, postal services and related matters. The CRA Act replaced the Broadcasting Act [Cap 72:04], the Telecommunications Act [Cap 72:03], and caused the amendment of the Postal Services Act to create a converged or an integrated regulatory authority for the communications industry. Under the Electronic Communications and Transaction Act the Authority has the responsibility of accrediting Secure Electronic Signature Service Providers. The Electronic Communications and Transactions Act No. 14 of 2014 (the Act) was enacted in 2014 and it commenced on 1st April 2016 with the passing of secondary legislation (Regulations). The Act and the Regulations are available at the BOCRA website www.bocra.org.bw.

In terms of section 10 of the Regulations, BOCRA is required to appoint an Independent Auditor/Auditing Firm that can audit Secure Electronic Signature Providers commonly known as Certification Authority (CA) and to perform periodic audits of the Accredited Certification Authority. The audit will be carried out to ensure the CAs are compliant with section 25 of the Act, regulations, Accreditation Certification Service standard and other obligations which BOCRA may prescribe from time to time.

The BOCRA Accreditation Certification Service Standard is based on the International Organization for Standardization ISO: 21188: 2006 ‘Public key infrastructure for financial services — Practices and policy framework’. In addition, the Audit will be carried out in accordance with Webtrust ‘Trust Service Principles and Criteria for Certification Authorities Requirements’, CA/Browser Forum “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly – Trusted Certificates”, and ETSI TS 101 456, the “Policy requirements for certification authorities issuing qualified certificates” will be recognised by BOCRA for accreditation.

BOCRA wishes to invite reputable, Independent Auditors\Auditing Firms to submit proposals demonstrating their capabilities and technical skills to carry out compliance audit in accordance with the ISO: 21188: 2006 or Webtrust Trust Service Principles and Criteria for Certification Authorities Requirements or

1 Webtrust “Trust Service Principles and Criteria for Certification Authorities Requirements” accessed at the following URL: http://www.webtrust.org/principles-and-criteria/item83172.aspx

2 CA/Browser Forum “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly” accessed at the following URL: https://cabforum.org/baseline-requirements-documents/
CA/Browser Forum “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly” or ETSI TS 101 456, the “Policy requirements for certification authorities issuing qualified certificate”.

1.2 Scope of Work

BOCRA is looking for reputable and qualified Independent Auditors/Auditing Firm to carry out specified audits for Public Key Infrastructure (PKI).

The selected auditors will be available for appointment for a period of 3 years unless either party terminates the agreement by notice.

The Scope of Work will focus primarily on and be guided by the BOCRA Accredited Certification Service Standards (Annexure 1), and Accredited Certification Standards Compliance Checklist (Annexure 2). As such Auditors are requested to go through both documents to determine the amount of work potentially involved in auditing a CA.

The auditor/auditing firm should be suitably qualified to perform the task at hand due to its specialised nature. The auditor/auditing firm should demonstrate, in addition to auditing competencies, specialised legal knowledge on issues such as the Act, Regulations, BOCRA Accredited Certification Service Standards and Certification Practices Framework, and other relevant standards.

BOCRA will pre-approve one or more auditing firms that it is satisfied can perform the said audit/s satisfactorily. The audit of an applicant CA will be carried out upon request of the Authority.

There will be two types of Audit Services;

1. Initial audit for CA applications: this is where proposals and/or applications for accreditation will be audited to determine whether an applicant meets all BOCRA’s requirements for a CA. The process is such that The Applicant will select the approved panel of Auditors/firms.

2. Periodic audits for Accredited CA’s: Annual audits for the period of the license.

In addition to the usual auditing team requirements, the team should also comprise of technical experts with experience in certification practices and procedures, Public Key Infrastructure (PKI), biometrics, cryptography, and related technologies used for authentication and certification. The auditing firm should be readily available to perform an audit as and when BOCRA requires its services within agreed time frames. The auditor should clearly state in the bid how long it will take to mobilise resources for an Audit when required by the Authority.
The audit team shall audit the CA and the trust service(s) it provides, covered by the defined scope against all applicable audit requirements.

The Auditor shall ensure that the scope and boundaries of the trust services of the CA are clearly defined in terms of the characteristics of the business, the organization, facilities, assets and technology.

The Auditor shall ensure that the CA's information security risk assessment and risk treatment properly reflect its activities and extend to the boundaries of its trust services activities.

The Auditor shall ensure that interfaces with services or activities that are not completely within the scope of the services are included in the CA's information security risk assessment.

The documentation of the Auditor shall include the policies and procedures for implementing the audit process, including checklists used in the audit, and the procedures for assessing the conformity of the CA and the trust services it provides with the criteria against which the audit is carried out.

The appointed Auditor shall audit the authentication service provider or its authentication products or services in accordance with the Act, Regulations and guidelines issued by the Authority from time to time.

An Auditor shall further:

(a) Use appropriate techniques to perform the audit;

(b) Evaluate the reliability and quality of the systems used, the integrity, confidentiality and availability of data as well as the compliance with the specifications included in any procedure’s manual and the security plan approved by the Authority, which shall at least comply with BOCRA Accredited Certification Service Standards;

(c) Verify that trustworthy systems contemplated in the Act and Regulations are used;

(d) Issue a report with the findings, conclusions and recommendations in each case.

Additional responsibilities that may be required of the Auditor by the Authority, include:
(a) following up on the audits in order to determine whether the authentication service provider has implemented the corrective actions suggested in the recommendations;

(b) issuing additional reports;

(c) taking part in contingency plan simulations; and

(d) furnishing additional copies of all reports issued to the Authority.

Upon conclusion of the Audit process, the Auditor shall provide a decision. The audit decision can be of one of the following three natures:

a) **Passed**: the audited trust service fulfils the criteria and is certified conformant;

b) **Failed with severe non-conformities**: the audited trust service is not certified conformant; or

c) **Passed with pending non-conformities**: successful audit status is conditional upon the implementation of corrective actions at least within 3 months in function of the type and criticality of the correction(s).

1.2.1 Application Review

Upon receiving an Audit application, the Auditor shall conduct a review of the information obtained to ensure that:

a) the information about the client and the product is sufficient for the conduct of the audit process;

b) any known difference in understanding between the Auditor and the client is resolved, including agreement regarding standards or other normative documents;

c) the scope of the audit sought is defined;

d) the means are available to perform all evaluation activities;

e) the Auditor has the competence and capability to perform the certification activity.

1.2.2 Contract Review

For each CA, the Auditor shall ensure that it does not accept any application for which it is not competent or otherwise unable to carry out the audit. The Auditor
shall then review the contract with the CA based on the results of this competence analysis. In particular, the Auditor shall be able to demonstrate that it has the competence to complete the following activities:

a) understand the areas of activity of the CA and the associated business risks;

b) define the competencies needed in the Auditor to certify, in relation to the CA identified activities, to the concerned trust services it provides, and to the relevant security risks, vulnerabilities and impacts on the CA; and

c) confirm the availability of the required competences.

1.2.3 Audit Report

1.2.3.1 Report Contents

The audit report provided to BOCRA and any other party that has a legal reason for viewing the report shall contain the following information:

a) an account of the audit including a summary of the document review and the standard(s), publicly available specifications and/or regulatory requirements against which the audit is carried out;

b) an account of the audit of the CA's information security risk analysis;

c) total audit time, and detailed specification of time spent on document review, assessment of risk analysis, on-site audit, and audit reporting; and

d) audit enquiries which have been followed, rationale for their selection, and the methodology employed including sampling methodology and test procedures.

1.2.3.2 Report Contents Details to be provided

The CA audit report of findings provided by the audit team leader to the Auditor shall be of sufficient detail to facilitate and support a certification decision and shall contain:

a) areas covered by the audit, including the certification requirements and the sites that were audited, the significant audit trails followed and the audit methodologies utilized;

b) observations made on the internal control environment including the strengths and weaknesses;
c) details of any nonconformities identified, supported by objective evidence and a reference of these non-conformities to the criteria against which the audit has been carried out; and

d) comments on the conformity of the CA and the trust services it provides with the criteria against which the audit has been carried out, together with a clear statement of nonconformity, and, where applicable, any useful comparison with the results of previous audits of the CA and of the concerned trust services. Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the audit report. If these methods are used, these documents shall be submitted by the audit team leader to the Auditor as evidence to support the certification decision. Information about the samples evaluated during the audit should be included in the audit report, or in other certification documentation. The report shall consider the adequacy of the internal controls and procedures adopted by the CA to give confidence in the trust services.

1.2.3.3 Programme of Periodic Surveillance

If requested by BOCRA, the Auditor should define a programme of periodic surveillance and re-assessment that includes on-site audits to verify that CA and trust services they provide continue to comply with the requirements.

The following activities should be part of the programme:

a) review of actions taken on non-conformities identified during the previous audit;

b) review of the multi-site sampling strategy, if sampling was applied in the previous audit;

c) review of any changes in documentation and CA operation;

d) review of internal audits and management review;

e) treatment of complaints;

f) use of marks and/or any other reference to conformity assessment; and

g) review of any public CA's statements with respect to its operations (e.g. promotional material, website).

Surveillance audits need not necessarily be full system audits. They shall be planned together with other surveillance activities and shall consider a previously applied multisampling strategy.
In addition, a sample of records relating to the operation of CA over the historical period since the previous audit shall be examined by the Auditor.

Surveillance reports should contain audit information on clearing of nonconformities revealed previously.

1.3 Eligibility

The Auditors/Firms should be registered in Botswana. In the case of Partnership, one of the them must be registered in Botswana.

1.4 Team Experience and Skills

1.4.1 Team Competencies

The Audit firm’s personnel performing audit shall have the following specific competences:

- formal academic qualifications or professional training or extensive experience indicating general capability to carry out complex tasks in an intelligent manner;

- at least four years full time practical workplace experience in Information Technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security, and physical security;

- knowledge of audit principles, practices and techniques in the field of CA audit gained in a training course of at least five days;

- knowledge of the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security;

- knowledge of the applicable standards, publicly available specifications and regulatory requirements for CA, and other relevant publicly available specifications including standards for IT product evaluation;

- Technical expertise in the area from either a full-time member of the Audit team or one that is engaged as and when needed.

Audit teams shall be competent with the duties assigned to them. The following requirements shall apply to the audit team as a whole. In each of
the following areas at least one auditor in the team shall satisfy auditors' criteria for taking responsibility within the audit team:

- managing the team (lead Auditor);
- demonstrated knowledge of the legislative and regulatory requirements and of legal compliance in the particular field of CA and information security;
- demonstrated knowledge of the current technical state-of-art regarding CA and Public Key Infrastructure;
- demonstrated knowledge in technologies applicable to the CA trust service being audited;
- demonstrated knowledge of performing information security related risk assessments so as to identify assets, threats and the vulnerabilities of the CA and understanding their impact and their mitigation and control; and
- demonstrated knowledge of organizational reliability issues. The audit team should be competent to trace indications of security incidents in the CA operations back to the appropriate elements of the CA controls.

An audit team may consist of one person provided that the person meets all criteria set out above. In addition to the above the Audit Team Leader must also have acted as an Auditor in at least three complete CA audits as well as demonstrate that they possess adequate knowledge and attributes to manage the audit process.

BOCRA is seeking proposals on how the auditing firm will set up an auditing team managed by a Lead Auditor. The members of the team should have both the skill and experience necessary to undertake the range of tasks set out in this Terms of Reference and these should be clearly displayed in the bid.

All team members must be personally available to do the work as and when required. The Lead Auditor will be held accountable, in terms of the tender and contract, for ensuring project deliverables and the professional conduct and integrity of the team. Where there are personnel changes, the Auditor is responsible of requesting approval from BOCRA for the change.
1.4.2 Team Experience Documentation

Bidders shall also include the following information in their Technical Proposal:

1.4.2.1 The Bidder shall use the CV template/form enclosed to provide:

- A detailed CV of the Project Manager and key members of the Bidder’s team;
- CVs of all team members must indicate their nationality and identification numbers.
- Experience of the team members in performing the requested Services;

1.4.3 Skills Transfer

Where the bidder will be utilising non-local skills, the bidder shall outline plans on how skills transfer and training of local staff shall be carried out. The auditing team will therefore be a specialised team of experts and should preferably in time comprise of mainly local experts.

Bidders should state how they intend to share knowledge to the rest of the local field, this could include but not limited to arranging and participating in training courses, provided that these courses relate to CA, security controls or auditing.

1.4.4 Talent Management

The Auditor shall establish, implement and maintain a procedure for management of competencies of personnel involved in the audit process. The procedure shall require the Auditor to:

- determine the criteria for the competence of personnel for each function in the audit process, taking into account the requirements of the schemes;
- identify training needs and provide, as necessary, training programmes on audit processes, requirements, methodologies, activities and other relevant audit scheme requirements;
- demonstrate that the personnel have the required competencies for the duties and responsibilities they undertake;
- formally authorise personnel for functions in the audit process;
- monitor the performance of the personnel.
1.4.5 Training

The Auditor shall have criteria for the training of audit teams that support the ability to demonstrate competence in:

- knowledge of the CA standards and other relevant publicly available specifications;
- understanding of trust services and information security including network security issues;
- understanding of risk assessment and risk management from the business perspective;
- technical knowledge of the activity to be audited;
- general knowledge of regulatory requirements relevant to CA; and
- knowledge of security policies and controls.

1.5 Organisation experience

1.5.1 The bidding company must also submit the following particulars:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>i)</td>
<td>Name of the Company and its physical and postal Addresses</td>
</tr>
<tr>
<td>ii)</td>
<td>Name of the Directors and Shareholders</td>
</tr>
<tr>
<td>iii) (a)</td>
<td>Registration No.</td>
</tr>
<tr>
<td></td>
<td>(b) Licence No. and attached copy</td>
</tr>
<tr>
<td>iv)</td>
<td>Date of Incorporation</td>
</tr>
<tr>
<td>v)</td>
<td>Present strength of the company (human resources, financial and others)</td>
</tr>
<tr>
<td>vi)</td>
<td>Recent list of the Companies and other Institutions at which you have rendered similar services (attach list separately)</td>
</tr>
<tr>
<td>7)</td>
<td>an overview of the company structure covering subsidiary companies, holding companies, financial backers.</td>
</tr>
<tr>
<td>8)</td>
<td>The locations of depots, agents and service centres appropriate to the supply of the services outlined in this document shall be included in this overview.</td>
</tr>
<tr>
<td>9)</td>
<td>Where response is being submitted by a group of companies or the prime contractor, the relevant details for each of the partners or sub-contractors should also be submitted in a manner similar to the main bidder. However, it must be noted that the full responsibility of the work will be with the main bidder.</td>
</tr>
</tbody>
</table>
In a case where the Audit firm is bidding as a Joint Venture with another entity or has outsourced some functions to an external entity, the Audit Firm should clearly state which roles each entity would be responsible for. **The Audit firm shall be responsible for all activities outsourced to another entity.**

1.6 Methodology

1.6.1 The bidder shall provide a proposal setting out its methodology, including the manner in which the Services are to be provided to ensure that the deliverables and any requirements of the Terms of Reference are met. At minimum, the bidder is expected to provide their Audit process approach that would show how the plan for and the date of the audit shall be agreed to with the CA. The Auditor may adopt reporting procedures that suit its needs but as a minimum these procedures shall ensure that:

- a meeting takes place, prior to leaving the CA's premises, between the audit team and the CA's management to which the audit team provides:
  - a written or oral indication regarding the conformity of the CA and the trust service(s) it provides with the criteria against which the audit has been carried out, and
  - an opportunity for the CA to ask questions about the findings and their basis; and
- the audit team leader provides the Audit firm with a report of its findings as to the conformity of the CA and the trust service(s) it provides with the criteria against which the audit has been carried out.

The Auditor shall have procedures, which are able to verify if the CA has established an audit programme or passed other external audits or certifications for the different sites, providing enough evidence that all site relevant requirements, specified in the criteria against which the audit is carried out, are fulfilled.

The Auditor's audit procedures shall not presuppose a particular manner of implementation of a trust service or a particular format for documentation and records.

Audit procedures shall focus on establishing that a CA and the trust service(s) meet the requirements specified in the criteria against which the audit is carried out.

The audit plan shall identify both the computer assisted auditing techniques and the network-assisted auditing techniques that will be utilized during the audit, as appropriate.
NOTE: Network assisted auditing techniques can include, for example, teleconferencing, web meeting, interactive web-based communications and remote electronic access to the trust service documentation and/or trust service processes.

The bidder shall include in their proposal all aspects of quality assurance of the proposed deliverables.

1.7 Fees

BOCRA is seeking proposals for an affordable auditing process. The bidder should specify its estimated audit costs in Botswana Pulas for initial and periodic audits inclusive of relevant taxes: including hourly rates, and possible expenses. The Auditing fees will be paid by the Applicant or the accredited company.

Bidders may specify any ancillary Services that they are able to provide that will add value to the Services requested in this EOI or which the bidder believes are necessary for this tender.

The cost of the Ancillary Services shall be shown separately in the Financial Proposal.

The Auditor shall have adequate arrangements (e.g. insurance or reserves) to cover liabilities arising from its operations. It shall also have the financial stability and resources required for its operations.

1.8 Evaluation Criteria

1.8.1 Scores for the Technical Evaluation

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Maximum Points</th>
<th>Attainable Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifications [Assess whether proposed bid meets tender specifications]</td>
<td>25 points</td>
<td></td>
</tr>
<tr>
<td>Organisational Capability &amp; Experience [marks to be awarded on evidence of bidder having undertaken similar projects, market experience, reputation, references]</td>
<td>20 points</td>
<td></td>
</tr>
<tr>
<td>Team Experience [assess level of relevant qualifications and experience]</td>
<td>20 points</td>
<td></td>
</tr>
<tr>
<td>Approach and Methodology</td>
<td>25 points</td>
<td></td>
</tr>
</tbody>
</table>
### 1.8.2 Citizen Participation

Bidders must define the level of citizen involvement in this tender by clarifying the citizens' roles. Non-citizen companies partnering with citizen companies and or individuals should clearly define the roles of the citizens in their bidding team.

Each bidder must indicate clearly the nationality of its Shareholders, Directors, Audit Partners, and team members. In addition, the bidder must enclose the proof of citizenship for its Shareholders, Directors Audit Partners, and team members e.g. Omang or passport.

A maximum of ten (10) points will be awarded to each bidder based on the level of participation of citizens in the project. The points shall be awarded in the following manner for citizen team members with technical responsibility in the tender,

- 0% citizen participation in project team = 0 points
- >0 – 50% citizen team members = 1-4 points
- >50% - 75% citizen team members = 5-7 points
- >75% - 100% citizen team members = 8-10 points

### 2. Contact Person

Interested organisations requiring clarification should write to the Procurement Department:

Ms Katlego Ramputswa  
Email: procurement@bocra.org.bw  
Tel: 3957755/3685500  
Fax: 3957976

### 3. Bid Submission Requirements

Bidders responding to the invitation must submit audit proposals that should at least contain the following information:

- Description of the process the auditor will follow in performing the initial audit of an applicant, and performing periodic audits.

- Time required to finalise initial audit, and periodic audits.
• Layout/structure of audit reports.

• Proposals on how to successfully structure the legal relationship between BOCRA, Auditor and Applicant to avoid litigation and ensure payment of the Auditor by the Applicant.

• The resources that will be utilised to perform the audits.

• Any other information in support of or to elucidate the proposal.

• Knowledge, experience and skills of proposed team.

The bid should include curricula vitae of all personnel whom the bidder proposes to use in carrying out the audits.

The bidder should submit a Project comprehension and management plan, setting out:

• Its understanding of the Terms of Reference;
• How the bidder proposes to manage the set of deliverables outlined in the Terms of Reference;
• A proposed Work Plan with time-table regarding the audits and reports;
• How the auditing team members will be supervised;
• How reporting to the Project Officer, in addition to the written report following the audit, will take place;
• Any innovative ideas for how the whole assignment can best achieve its objectives.

4. Submission Format

Proposals should be bound and enclosed in an envelope clearly marked to the attention of BOCRA as follows:

BOCRA/PT/008/2017.18
PROVISION OF AUDIT SERVICES FOR SECURE ELECTRONIC SIGNATURE PROVIDERS TO BOTSWANA COMMUNICATIONS REGULATORY AUTHORITY

Postal Address
Botswana Communications Regulatory Authority
Private Bag 00495
Gaborone
**Physical Address**
BOCRA Head Office
Plot 50671, Independence Avenue

5. **Deadline**

Proposals should be hand delivered to BOCRA Head Office on or before **10:00hrs** on **Friday 8th December 2017**.

6. **Acknowledgement**

6.1 Proposals will be assessed and responses will only be sent to applicants who would have submitted by the closing date.

6.2 Nothing in this invitation is to be construed as creating any binding contract.