Statutory Instrument No. 42 of 2016

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT
(ACT NO. 14 OF 2014)

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS REGULATIONS, 2016

(*Published on 8th April, 2016*)

ARRANGEMENT OF REGULATIONS

REGULATION

IN EXERCISE of the powers conferred on the Minister of Trade and Industry by section 47 of the Electronic Communications and Transactions Act, the following Regulations are hereby made —

Citation

1. These Regulations maybe be cited as the Electronic Communications and Transactions Regulations, 2016.

Interpretation

2. In these Regulations, unless the context otherwise provides —

"accreditation" means accreditation granted under regulation 4;

"accredited certification service provider" means a certification service provider accredited under these Regulations;

"ACS Compliance Checklist" means the Accredited Certification Service Standards published by the Communications Regulatory Authority for compliance audit purposes;

"ACS Standards" means the Accredited Certification Service Standards;

"certification practice statement" means a statement issued by a certification service provider specifying the process of issuing certificates;

"Communications Regulatory Authority" means the Communications Regulatory Authority established under section 3 of the Communications Regulatory Authority Act;

Cap. 72:03

"key personnel" means employees who have direct responsibility for the day to day operations, security and performance of a certification service provider, or whose duties directly involve the issuance, renewal, suspension, revocation of certificates, the process of identification of any person requesting a certificate, the creation of private keys or the administration of the certification service providers computing facilities;

"qualifying certificate" means a certificate which conforms with the requirements set out in Schedule 2;

"qualifying certification service provider" means a certification service provider who satisfies the requirements set out in Schedule 2;

"qualifying signature verification device" means a signature creation service which conforms with the requirements set out in Schedule 2;

"signatory" means a person who holds a signature creation device and acts either on his or her own behalf or on behalf of another person;

"signature creation data" means unique data such as codes or private cryptographic keys used by the signatory to create an electronic signature;

"signature creation device' means configured software or hardware used to implement the signature creation data;

"signature verification data" means data such as codes or public cryptographic keys used for the purpose of verifying an electronic signature; and

"standard end-user agreement" means an agreement between the accredited certification service provider and its customer for the provision of secure electronic signatures.

Application for registration as certification service provider

3. (1) A person who wishes to operate as a certification service provider shall make an application for accreditation to the Communications Regulatory Authority in Form A set out in Schedule 1, accompanied by a non-refundable fee of P10 000.

(2) Any person who has been operating as a certification service provider shall notify the Communications Regulatory Authority within six months from the coming into operation of these Regulations.

(3) A certification service provider who contravenes any provision of this regulation is liable to a fine not exceeding P5 000.

Issuance of certificate

4. (1) The Communications Regulatory Authority shall where an application made under regulation 3 meets all the requirements, issue a certificate of accreditation in Form B set out in Schedule 1.

(2) An accreditation certificate issued in terms of this regulation shall be valid for a period of two years.

(3) A certification service provider shall, at all times, display a certificate of accreditation issued under subregulation (1) in a conspicuous manner in its place of business.

Renewal of certificate

5. (1) An accredited certification service provider shall not later than three months before the date of expiry of the accreditation make an application to the Communications Regulatory Authority for the renewal of accreditation.

(2) An application for renewal shall be made to the Communications Regulatory Authority in Form A set out in Schedule 1 and shall be accompanied by —

(*a*) a renewal fee of P5 000;

(*b*) the latest version of the certification practice statement;

(*c*) a copy of the latest version of the standard end-user agreement;

(*d*) the audited financial statements of the two previous years;

(*e*) an audited report; and

(*f*) any other information as the Communications Regulatory Authority may request.

(3) The Communications Regulatory Authority may grant a renewal certificate for accreditation where it is satisfied that the applicant —

(*a*) meets the requirements of these Regulations; and

(*b*) has complied with conditions imposed on the accreditation.

(4) An application for renewal shall be considered by the Communications Regulatory Authority within two months from the date of submission of the application.

Refusal to grant or renew accreditation

6. (1) The Communications Regulatory Authority may refuse to grant or renew accreditation where —

(*a*) the certification service provider –

(i) has not complied with any provisions of the Act or of these Regulations or of the ACS Standards,

(ii) has not provided the Communications Regulatory Authority with the requested information for the application or the renewal of accreditation,

(iii) is wound up or liquidated, or

(iv) has within a period of 10 years immediately preceding the date of his or her accreditation been convicted, whether in Botswana or elsewhere of an offence involving fraud or dishonesty or has been convicted of an offence under the Act or these Regulations;

(*b*) it is not satisfied with —

(i) the qualifications or experience of the certification service provider's key personnel,

(ii) the financial standing of the certification service provider or of its significant owners, or

(iii) the record of past performance or expertise of the certification service provider or of its personnel;

(*c*) it has reason to believe that the certification service provider may not be able to act in the best interest of its subscribers or customers having regard to the reputation, character, financial integrity and reliability of the certification service provider or any of its significant owners or key personnel;

(*d*) the certification service provider or any of its owners or key personnel is found guilty of misconduct of business; or

(*e*) it is of the opinion that it is in the interest of the public to do so.

(2) The Communications Regulatory Authority shall inform the certification service provider of the reasons to refuse to grant or renew accreditation.

Revocation, suspension or cancellation

7. The Communications Regulatory Authority may revoke, cancel or suspend accreditation of a certification service provider —

(*a*) where it is of the view that the information provided is false, misleading or inaccurate;

(*b*) where the certification service provider —

(i) fails to undergo an audit required under regulation 15 (1),

(ii) is likely to be wound up,

(iii) fails to carry on the business for which it was accredited, or

(iv) contravenes or fails to comply with any condition in respect of its accreditation;

(*c*) where the Communications Regulatory Authority has reason to believe that the certification service provider or any of its key personnel has not performed their duties efficiently, honestly or fairly; or

(*d*) upon receipt of a written request by the certification service provider to cancel, revoke or suspend the accreditation.

Appeal

8. Any person aggrieved by the decision of the Communications Regulatory Authority may within thirty (30) days of the decision appeal to the High Court.

Recognition of secure electronic signatures

9. (1) A certification service provider who wishes to provide products or services required to authenticate and recognise secure electronic signatures shall make an application for accreditation to the Communications Regulatory Authority in Form A set out in Schedule 1, accompanied by —

(*a*) a non-refundable fee of P10 000;

(*b*) the service providers certification practice statement and certification policy;

(*c*) a copy of the standard end-user agreement;

(*d*) a business plan;

Cap. 61:05

(*e*) the audited financial statements from the two previous years issued by an auditor appointed under the Accountants Act; and

(*f*) any other information as the Communications Regulatory Authority may request.

(2) The Communications Regulatory Authority shall consider an application made under subregulation (1) within three (3) months of receipt of the application.

(3) Where the Communications Regulatory Authority has requested for additional information or any clarification, the three months for consideration of the application shall run from the date of the submission of the additional information.

(4) The Communications Regulatory Authority may award accreditation subject to such conditions as it may deem fit.

10. (1) An accredited certification service provider shall provide an audit report compiled by an auditor appointed by the Communications Regulatory Authority. Audit report

(2) All fees relating to the audit report shall be borne by the certification service provider.

(3) The audit report shall, confirm in respect of —

(*a*) an electronic signature that it —

(i) conforms with the requirements of section 25 of the Act and is capable of identifying the signatory,

(ii) is created by qualifying signature creation and signature verification devices,

(iii) is based on a qualifying certificate, and

(iv) complies with the international standards with which the certification service provider claims in its application for accreditation; and

(*b*) a certification service provider that it —

(i) satisfies the requirements set out in Schedule 2,

(ii) has systems in place to ensure compliance with the Act and these Regulations,

(iii) has sufficient financial resources to provide for professional indemnity or insurance cover, and

(iv) has personnel who satisfy the requirements set out in Schedule 2.

11. (1) An accredited certification service provider shall prepare a certification practice statement in accordance with the ACS standards. Certification of practice statement

(2) Any change to the certification practice statement shall require prior written approval of the Communications Regulatory Authority.

(3) A copy of the latest version of the certification practice statement, together with its effective date, shall be filed with the Communications Regulatory Authority and published on the certification service provider's website accessible to members of the public.

(4) A certification service provider shall log all changes to a certification practice statement together with the effective date of each change.

(5) An accredited certification service provider shall keep in a secure manner a copy of each version of the certification practice statement together with the date it came into effect and the date it ceased to have effect.

12. (1) The Communications Regulatory Authority shall keep and maintain a register of all accredited certification service providers. Maintenance of register

(2) The register under subregulation (1) shall provide —

(a) the name and address of the certification service provider;

(*b*) a description of the certification service provider; and

(*c*) a list of accredited certification service providers recognised by the Communications Regulatory Authority.

(3) The Communications Regulatory Authority shall publish the register on its website or by any other means it deems fit for access by the public.

13. An accredited certification service provider shall ensure that its business is conducted in compliance with — Conduct of business

(*a*) the provisions of the Act and these Regulations;

(*b*) the ACS standards; and

(*c*) any condition of its accreditation.

Change in ownership, management, etc. of certification service provider

14. (1) An accredited certification service provider that wishes to change its ownership, management or operations shall make an application to the Communications Regulatory Authority for its approval.

(2) Upon receipt of an application under subregulation (1), the Communications Regulatory Authority may –

(*a*) request the certification service provider to submit an audit report; or

(*b*) suspend or cancel the accreditation of the service provider.

(3) Where an audit report is requested, all expenses shall be borne by the certification service provider.

(4) Where the Communications Regulatory Authority has authorised a change in the ownership or management of a certification service provider, it shall publish a copy of the latest certification practice statement of the certification service provider.

Review and audits

15. (1) The Communications Regulatory Authority shall monitor the conduct, systems and operations of an accredited certification service provider to ensure that it complies with the Act and these Regulations and where necessary –

(*a*) require an accredited certification service provider to undergo an audit if it is of the opinion that —

(i) a significant change in the ownership or operations of the accredited certification service provider has occurred, or

(ii) such audit is reasonably required or is otherwise necessary;

(*b*) issue such direction to the accredited certification service provider for compliance as it deems necessary; or

(*c*) temporarily suspend or cancel accreditation.

(2) Where an audit is required in terms of subregulation (1) (*a*), an accredited certification service provider shall at its own expenses commission an audit report to be compiled by an auditor appointed by the Communications Regulatory Authority which shall be completed within such period as may be specified.

Inquiry into allegations of misconduct etc.

16. (1) The Communications Regulatory Authority may inquire into any allegations that —

(*a*) a significant change in the ownership, management of operations of an accredited certification service provider has occurred, the notification of which has not been granted in terms of regulation 14;

(*b*) an employee of an accredited certification service provider has committed an act which may render him or her guilty of misconduct and unfit to continue with the service of the certification service provider;

(*c*) an accredited certification service provider has contravened the provisions of the Act or of these Regulations; or

(*d*) an accredited certification service provider is in breach of its certification practice statement or the terms of its standard end-user agreement.

(2) If, after inquiring into an allegation made under subregulation (1) and having given the accredited certification service provider an opportunity to be heard, the Communications Regulatory Authority is of the opinion that the allegation is proven, it shall take action in accordance with regulation 17.

(3) If the Communications Regulatory Authority is of the opinion that the allegation under subregulation (1) is made in bad faith, it may require the person who made the allegation to be liable for the costs related to the inquiry including costs of an audit that may be required.

Take-down notifications

17. (1) Where a take-down notification is received by the Communications Regulatory Authority in terms of section 44 of the Act, it shall —

(*a*) verify the identity of the complainant;

(*b*) ensure that the take-down notification complies with section 44 of the Act;

(*c*) send the take-down notification to the certification service provider identified by the complaint in the take-down notification; and

(*d*) keep a record of the take-down notification, action taken and reports received from the certification service provider in accordance with subregulation (2).

(2) Where a certification service provider receives a take-down notification in terms of section 44 of the Act, it shall within seven (7) days of receipt of the take-down notification submit a report to the Communications Regulatory Authority regarding the action taken.

(3) A certification service provider who fails to provide a report in accordance with subregulation (2), shall be liable to a fine not exceeding P5 000 or to imprisonment for a term not exceeding six (6) months, or to both.

(4) The Communications Regulatory Authority shall administer a take-down notification where a certification service provider identified by the complaint in the take-down notification –

(*a*) is registered in Botswana; or

(*b*) has its main operations of service carried out of Botswana.

(5) The Communications Regulatory Authority shall not in response to a notification of unlawful activity be liable for any wrongful take-down notification by a certification service provider.

Complaints relating to contravention of Act

18. (1) A complaint by a consumer in relation to an alleged contravention of Part VI of the Act shall be referred to a competent authority responsible for consumer protection.

(2) A complaint made by a person in relation to the contravention of Part VII of the Act shall be referred to a competent authority.

SCHEDULE 1

FORM A
(regulations 3 (1), 5(2), 10(1))

APPLICATION FORM FOR ACCREDITATION/ RECOGNITION/RENEWAL FOR CERTIFICATION SERVICE PROVIDERS

BOCRA

The application form is for Certification Service Providers who desire to be accredited, recognised or renew their accreditation, under the Electronic Communications and Transactions Regulations ("Regulations") made under the Electronic Communications and Transactions Act. The applicants are required to comply with the Accredited Certification Standards (ACS) issued by Botswana Communications Regulatory Authority (BOCRA)

SECTION 1: PARTICULARS OF THE APPLICANT

1.1 Applicants Details

Company Name:	
Physical Address:	
Postal address:	
Telephone:	
Facsimile:	
Mobile:	
Email:	

1.2 Contact Person Details (Official Communication)

Name:	
Designation:	
Physical Address:	
Postal Address:	
National I.D / Passport No.	
Telephone: (Work) (Res)	
Email Address	
Facsimile:	
Mobile:	
Email:	

1.3 Company Registration

State whether company is:

Public Limited

Private Limited

Owned 100% by Government

Others (please specify):

Main business activity	
Company website (URL)	

The following information should be attached:

(*a*) Company registration certificate, where the applicant company is a subsidiary of another company, information about the parent and ultimate holding companies (the entire group structure) must be provided; and

(*b*) A certified true copy of the applicant company's resolution(s):

(i) to apply for accredited or recognition as Certification Service Provider, or (in the case of an accredited secure digital signature provider applying for renewal of its accreditation) for renewal of its accreditation, and

(ii) to authorise, for the purpose of making this application on the applicant company's behalf, the person(s) making the application.

1.4 Ownership

Provide names, addresses and contact details of Directors/ Board Members:

Name of Company/Individual	
Country of Incorporation/ Nationality	
National I.D/Passport No.	
Physical Address	
Postal Address	
Share %	

Name of Company/Individual	
Country of Incorporation/ Nationality	
National I.D/Passport No.	
Physical Address	
Postal Address	
Share %	

Please attach Shareholder Certificates

1.5 Management Structure

Provide the details of the key executive management

Name:	Name:
Designation:	Designation:
Physical Address:	Physical Address:
Postal Address:	Postal Address:
National I.D/ Passport No.	National I.D/ Passport No.
Telephone: (Work) (Res)	Telephone: (Work) (Res)
Facsimile:	Facsimile:
Mobile:	Mobile:
Email:	Email:

Provide the curriculum vitae for the key personnel. The applicant is required to provide contact details of the key personnel as per the ACS Standards.

Name:	Name:
Designation:	Designation:
Physical Address:	Physical Address:
Postal Address:	Postal Address:
National I.D/ Passport No:	National I.D? Passport No:
Telephone: (Work) (Res)	Telephone: (Work) (Res)
Facsimile:	Facsimile:
Mobile:	Mobile:
Email:	Email:

SECTION 2: FOREIGN RECOGNITION

2.1 Has the Applicant applied to the competent authority in another jurisdiction/country to become a recognised/accredited Certification Service Provider or its equivalent in that jurisdiction/country?

.....

.....

If yes, please state the result and the name of the jurisdiction/country. If the application is unsuccessful, please provide the reasons, if necessary submit a separate paper

.....

.....

.....

.....

.....

2.2 If the Applicant is accredited in another jurisdiction/country, a copy of the accredited certificate must be provided.

.....

.....

SECTION 3: LEGAL PROCEEDINGS INFORMATION

3.1 Has the applicant ever been involved in any legal proceeding or dispute settlement in Botswana or elsewhere in its capacity as a Certification Service Provider?

Yes No

If the answer to the above question is "yes", please furnish complete details (please attach a separate sheet if the space provided is inadequate)

.....

.....

.....

.....

3.2 Has the applicant company or its substantial shareholder or any of their respective directors and key executives, or any of the trusted persons, ever been convicted of an offence for which the conviction involved a finding that it/he/she acted fraudulently or dishonestly?

Yes No

If the answer to the above question is "yes", please furnish complete details (please attach a separate sheet if the space provided is inadequate).

.....

.....

.....

SECTION 4: ANNEXURES

The Applicant should attach the following documents:

(*a*) Full technical description of the secure electronic signature system;

(*b*) Service provider's Certification Practice Statement and Certification Policy;

(*c*) Standard end-user agreement;

(*d*) Audited report in accordance with Accredited Certification Standards Compliance Checklist issued by the Authority;

(*e*) Privacy/security policy;

(*f*) Detail Business Plan covering the following:

(i) Profit and loss accounts, balance sheets and cash flow statements, target market, business strategy. All assumptions used e.g. asset depreciation policies, subscriber projections, budget and annual increase/decrease in operating expenditure shall be clearly explained;

(ii) Financial ratios including return on assets, return on equity, operating profit margin, net profit margin, current ratio, quick ratio and debt-equity ratio;

(iii) All capital expenditure and working capital requirements for the first five (5) years of operations;

(iv) Source of Funding;

(v) Proposed fee structure for the digital signatures;

(vi) Human Resource plan including the organisational chart, curriculum vitae of the key personnel,

(*g*) Incident Management plans and Disaster Recovery Plan;

(*h*) Audited Financial Report for the previous two (2) years.

SECTION 5: DECLARATION

1. In applying to the BOCRA to operate as an accredited/recognised Certification Service Provider under the Electronic Communications and Transactions Act and the Regulations, I declare that all the above information provided by the company is true and complete.

2. In the event that any of the information provided by the company is found to be false or misleading, the Authority reserves the right to take appropriate enforcement action against the company under the Act and/or the Regulations (including, without limitation, cancelling or suspending the accreditation of the company).

Applicant Name:.....

Signature: .....

Designation.....

Date:.....

Company Stamp:.....

FORM B
CERTIFICATE OF ACCREDITATION
(*regulation 4 (1)*

Communications Regulatory Authority, in the exercise of powers conferred upon it under Section 26(2) of the Electronic Communications and Transactions Act [No. 14 OF 2014], hereby grants a :

CERTIFICATION SERVICE PROVIDER ACCREDITATION

TO

Having its registered office at Plot ..... to offer services of providing secure electronic signatures to the public for a period of five (5) years, subject to the provisions of the Electronic Communications and Transactions Act, [No. 14 of 2014] and the CONDITIONS in Annexure 1 attached hereto and such regulations and conditions as have been or may be imposed from time to time.

The Licensee shall at all times display the licence in a conspicuous place at the licensee's registered offices.

Given under my hand and seal in .....this .....day of ..... 20.....

[Accreditation mark of the Communications Regulatory Authority]

.....
CHIEF EXECUTIVE

SCHEDULE 2

(*regulation 11*)

A. Requirements of Qualifying Signature Creation Devices

1. A qualifying signature creation device shall, by appropriate technical and procedural means, ensure as a minimum that -

(*a*) the signature creation data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;

(*b*) the signature creation data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology; and

(*c*) the signature creation data used for signature generation can be reliably protected by the legitimate signatory against use by others.

2. A qualifying signature creation device shall not alter the date to be signed or prevent such data from being presented to the signatory prior to the signature process.

B. Requirements for Qualifying Signature Creation Devices

1. During the signature-verification process it shall be ensured with reasonable certainty that:

(*a*) the date used for verifying the signature corresponds to the data displayed to the verifier;

(*b*) the signature is reliably verified and the result of that verification is correctly displayed;

(*c*) the verifier can, as necessary, reliably establish the contents of the signed data;

(*d*) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;

(*e*) the result of verification and the signatory's identity are correctly displayed;

(*f*) the use of a pseudonym is clearly indicated; and

(*g*) any security-relevant changes can be detected.

C. Requirements for Qualifying Certificates

1. A qualifying certificate shall contain –

(*a*) an indication that the certificate is issued as a qualifying certificate;

(*b*) the identification of the certification service provider and the jurisdiction in which it is established;

(*c*) the name of the signatory or pseudonym, which shall be identified as such;

(*d*) provision for a specific attribute of the signatory, if relevant, depending on the purpose for which the certificate is intended;

(*e*) signature verification data which corresponds to signature creation data under the control of the signatory;

(*f*) an indication of the beginning and end of the period of validity of the certificate;

(*g*) the identity code of the certificate;

(*h*) the advanced electronic signature of the certification service provider issuing it;

(*i*) limitations on the scope of use of the certificate, if applicable; and

(*j*) limits on the value of transactions for which the certificate can be used, if applicable.

D. Requirements for Qualifying Certification Service Providers

1. A certification service provider shall –

(*a*) be a fit and proper person to the satisfaction of the Communications Regulatory Authority;

(*b*) demonstrate the reliability and expertise necessary for providing certification services;

(*c*) demonstrate adherence or the ability to adhere to these Regulations;

(*d*) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

(*e*) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

(*f*) verify, by appropriate means, the identity and, if applicable, any specific attributes of the person to a certificate is issued;

(*g*) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(*h*) take measures against forgery of certificates, and in cases where the certification service provider generates signature creation data, guarantee confidentiality during the process of generating such data;

(*i*) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Act, and these Regulations, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(*j*) not store or copy signature creation data of the person to whom the certification services provider provided key management services;

(*k*) before entering into a contractual relationship with a person seeking a certificate to support his or her electronic signature, inform that person by a means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, shall be in writing. Relevant parts of this information shall also be made available on request to third-parties relying on the certificate; and

(*l*) use trustworthy systems to store certificates in a verifiable form so that –

(i) only authorised persons can make entries and changes,

(ii) information can be checked for authenticity,

(iii) certificates are publicly available for retrieval in only those cases for which the certificate holder's consent has been obtained, and

(iv) any technical changes compromising these security requirements are apparent to the operator.

E. Requirements for Key Personnel of Qualifying Certification Service Providers

1. A certification-service-provider shall ensure that its key personnel –

(*a*) are fit and proper persons to carry out the duties assigned to them; and

(*b*) have not within a period of ten (10) years preceding their employment been convicted, whether in Botswana or elsewhere, of –

(i) an offence involving fraud or dishonesty; or

(ii) an offence under the Act or these Regulations

2. Key personnel shall possess the relevant expert knowledge, experience, and qualifications necessary for the services provided, expertise in electronics signature technology and familiarity with prior security procedures, they shall also apply administration and management procedures which are adequate and correspond to recognised standards and shall possess knowledge of the Act and these Regulations.

MADE this 17th day of March, 2016.

VINCENT T. SERETSE,
Minister of Trade and Industry.