ACCREDITATION CERTIFICATION

SERVICE STANDARD, 2017

(ACS, 2017)

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

Table of Contents

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

Abbreviations & Definitions

"Accreditation"	Means accreditation granted under Regulation 4 of the Electronic Communications and Transactions Regulations, 2016;
"Act"	Means the Electronic Communication and Transactions Act.
"Auditor"	Means an independent audit firm appointed by the BOCRA in accordance with the Act and Regulations
"BOCRA"	Means the Communications Regulatory Authority established under section 3 of the Communications Regulatory Authority Act;
"Certification Authority" or CA	means Secure Electronic Signature Providers who satisfy the requirements of **Schedule 2 of the Regulations** in the manner detailed in these ACS Standards and accredited in accordance with Section 25 of the Act;
"Certification Practice Statement"	Means a statement issued by a Certification Authority (CA) specifying the process of issuing certificates.
"ETSI TS 101 456"	Means the European Telecommunications Standards Institute (ETSI) "Policy requirements for certification authorities issuing qualified certificates" issued by ETSI.
"ISO21188:2006"	Means International Standard Organisation (ISO) (Public key infrastructure for financial services - Practices and policy framework) issued by ISO.
"CA certificate"	Means a certificate which conforms to the requirements of **Schedule 2 of the Regulations** in the manner detailed in these ACS Standards.
"Signature creation device" (SCD)	Means a secure electronic signature creation device which conforms to the requirements of **Schedule 2 of the Regulations** in the manner detailed in these ACS Standards.

“Regulations”	Means the Electronic Communications and Transactions Regulations, 2016, (Statutory Instrument No. 42 of 2016).
“Signatory”	Means a person who holds a secure electronic signature creation device and acts either on his or her own behalf or on behalf of another person.
Significant owner	Means an individual or body corporate holding a shareholding of more than ten per cent (10%) of the voting rights in the Certification Authority.
“the ACS Standards”	Means the Accredited Certification Service Standards published by the Authority in accordance with **Regulations, Schedule 1**
“Trusted Personnel”	Means employees who have direct responsibilities for the day-to-day operations, security and performance of the 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 provider’s computing facilities.

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

1. Introduction

1.1 Electronic commerce developed globally at a fast pace to become a pre-eminent way of conducting business. The successful uptake of this way of doing business was a result of the internationalisation of markets and the realisation that through electronic commerce, one could not only purchase products and services that were not available in one's immediate location, but also market and sell products and services worldwide, thereby dramatically increasing the potential customer base for a business. The possibility for consumers to purchase from foreign jurisdictions and for producers to sell to foreign jurisdictions has also proved itself to be a formidable way of increasing competitive efficiency and has resulted in better standards of living for societies who have embraced this way of doing business.

1.2 Electronic Commerce prospects, however, are unachievable without a good underlying and enabling legal framework, based on international best practices. For this reason, the **Electronic Communications and Transactions Act** ("**the Act**") was enacted by Botswana in 2014, thereby giving the country a foundation from which to start capitalising on the opportunities offered by electronic commerce ("**e-Commerce**"). The Act, however, required a set of subsidiary legislation in order to properly give effect to certain elements of the principal legislation; thus, the **Electronic Communications and Transactions Regulations** ("**the Regulations**") Statutory Instrument No. 42 of 2016 has been published on 8th April 2016.

1.3 A major part of the Regulations deals with electronic signatures, a fundamental element of e-Commerce. Electronic signatures are vital because they provide the ability to identify the originator of an electronic document and to signify acceptance of the contents of that document in the same manner and at least to the same extent that this is possible with a traditional handwritten signature. Whilst the term 'electronic signature' is an extensive term which can incorporate any type of signature done in an electronic

BOTSWANA COMMUNICATIONS REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

manner, such as putting one's name at the bottom of an email message, or placing a scanned signature on an electronic document, not all electronic signatures have the same evidentiary value. For an electronic signature to be considered as equivalent to a handwritten signature, it needs to be secure in terms of **Article 25 of the Act**. This, in turn, means that it has to be accredited, under the Regulations, by BOCRA.

1.4 The accreditation of an electronic signature product/service is necessary if one is claiming outright that his electronic signature product/service can provide the same evidentiary weight as a handwritten signature. If one is providing an electronic signature product/service which is not accredited or otherwise recognised by BOCRA under the **Act** and **Regulations**, this will simply mean that, in the event of legal proceedings, his subscribers will have the burden of proving the reliability of the signature used in the circumstances at hand. On the other hand, an accredited secure electronic signature shifts the burden of proof in favour of the signatory, so that such a signature will be considered reliable unless clear evidence to the contrary is presented.

1.5 **Regulation 6(1)** states that the Authority shall only award accreditation of an electronic signature where it is satisfied that:

(a) the secure electronic signature –

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

(ii) is created by a qualifying signature creation device and verified by a secure signature-verification device, and

(iii) is based on a qualifying certificate;

(b) the certification service provider meets the requirements set out in Schedule 2;

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

1.6 These **Accredited Certification Service Standards** ("**ACS Standards**"), issued in accordance with **Regulations, Schedule 1** aim to further supplement the provision of the Act and the Regulations by providing details as to the standards that are to be achieved for a certification service provider to qualify for accreditation by BOCRA. **It is important to note that compliance with the Schedules in the Regulations is not to be interpreted in any manner except as detailed in these ACS Standards.**

1.7 The ACS Standards needed to be rigorous enough to enable a certification service provider accredited by BOCRA to meet the requirements imposed worldwide and are globally trusted online. The ACS Standards require a qualifying Certification Authority (CA) to be compliant with **ISO 21188: 2006** 'Public key infrastructure for financial services — Practices and policy framework' issued by the International Organization for Standardization (ISO). **Thus, in order to be accredited, a certification service provider must show that it abides by ISO 21188: 2006 in its entirety as well as the provisions in the following paragraphs**.[1]

1.8 In addition the Authority will recognise for accreditation Certification Authority which complies with **Webtrust** "Trust Service Principles and Criteria for Certification Authorities Requirements[2]", **CA/Browser Forum** "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly – Trusted Certificates[3]" and **ETSI TS 101 456,** the "Policy requirements for certification authorities issuing qualified certificates".

---

[1] *Note that whilst this does not mean that the service provider needs to be certified as compliant by ISO, such certification will mean that only the additional provisions in this document will need to be audited in accordance with Regulation 6.*

[2] *Webtrust "Trust Service Principles and Criteria for Certification Authorities Requirements" accessed at the following URL*: http://www.webtrust.org/principles-and-criteria/item83172.aspx

[3] *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/

BOTSWANA COMMUNICATIONS REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

1.9 It should be noted that the Regulations make reference to a "signatory" being "a person who holds a signature creation device and acts either on his or her own behalf or **on behalf of another person he or she represents**". In the latter scenario, one needs to distinguish between the person actually holding the signature creation device and the person/entity on whose behalf the 'holder' of the signature creation device is acting, as different requirements apply. For this purpose, the term "signatory" is being sub-divided into:

- the **subscriber,** that is, the person/entity on whose behalf the 'holder' of the signature creation device is acting as this is the person/entity actually contracting with the CA (for example, an employer);
- the **subject,** that is, the person/entity to whom the certificate applies (for example, an employee acting on behalf of an employer).

1.10 In terms of Se**ction 27(2) of the Act**, it is the signatory that bears liability for failing to comply with **Section 27(1) of the Act** towards the CA, a relying party or another third party, as the case may be.

2. Mandatory Requirements for CAs

2.1 General Requirements

2.1.1 Overarching Principles

2.1.1.1 The legitimacy of the certificates issued is dependent on the CA as a trusted party. It is therefore essential that the management of the CA is secure and proper. For this reason, a CA must abide by these ACS Standards, the Electronic Communications and Transactions Act, and the Electronic Communications and Transactions Regulations and any other prevailing legislation at all times.

BOTSWANA COMMUNICATIONS REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

2.1.1.2 In providing its services, the CA must operate in a manner that is fair, just and non-discriminatory and must, in the absence of a valid reason, make its services accessible to any applicant who requests them.

2.1.1.3 The CA's policies and practices shall be transparent and publicly-available, and any changes thereto shall be brought to the attention of any relevant party. Prior notice of intended changes must be given to all relevant parties at least one (1) month before such changes are effected.

2.1.1.4 The CA shall at all times ensure compliance with data protection legislation in Botswana when processing and storing information during the provision of its services. In particular, the CA must implement appropriate technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Information in the care of the CA must not be disclosed without the user's consent, unless this is done through an order of a court or tribunal.

2.1.1.5 The CA may outsource parts of its procedures, as long as the services provided by the subcontractor also meet the applicable requirements of the ACS Standards. A detailed agreement must be in place with all subcontractors and a copy of such agreements is to be provided to BOCRA. Additionally, details of the subcontractors' policies and practices must be clarified in the CA's Certification Practice Statement as detailed below. Notwithstanding such subcontracting arrangements, the CA shall remain responsible and liable for the provision of its services at all times.

2.1.2 Fit & Proper Persons

2.1.2.1 Upon application for accreditation and renewal of accreditation, BOCRA will carry out a due diligence exercise in order to ensure that persons involved with the provision of an accredited certification service:

2.1.2.1.1 are of good standing;
2.1.2.1.2 have the financial stability and resources to operate in conformity with the Act, the Regulations and these ACS Standards;
2.1.2.1.3 have adequate arrangements to cover liabilities arising from its operations and/or activities;
2.1.2.1.4 have the expertise to carry out their proposed operations as required under the Act, the Regulations and these ACS Standards.

2.1.2.2 Accreditation is only available to a body corporate; however it need not be resident, established or operating in or from Botswana, provided that it is complaint with the requirements of the Regulations[4] and Accreditation Application procedure. The intention behind this provision is to allow Botswana to be a jurisdiction of choice for providers who wish to obtain accreditation in a reputable jurisdiction outside of their country of establishment.

2.1.2.3 Where the audited financial statements of the CA applying for accreditation are not available (e.g. if the applicant is a newly-registered entity), then the applicant will need to satisfy BOCRA that it is able to comply with **Paragraphs 2.1.2.1.2 and 2.1.2.1.3** adequately, for example, through the provision of a bank guarantee.

2.1.2.4 In terms of **significant ownership** of the entity applying to be accredited as a certification service provider, BOCRA will take the

[4] Regulation and the Act allows for the Foreign Recognition of the Certification Authority.

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

following circumstances into account when deciding whether the applicant is 'fit and proper':

2.1.2.4.1 Where a significant owner is **an individual** and he/she:

- had been convicted of a crime which carries a penalty of imprisonment for a term exceeding four (4) years under the Laws of Botswana;
- refuses to give BOCRA any information requested;
- has been asked to resign from employment;
- has been dismissed from employment;
- has a history of bankruptcy;
- has a history of criminal activity;
- has requested undue levels of secrecy;
- resides in, is domiciled in, or has citizenship of, a jurisdiction that Botswana, or the Authority, has blacklisted.

2.1.2.4.2 Where a significant owner is an **entity** which:

- has been involved in some criminal activity;
- is structured in a manner, or if its nature makes it difficult to identify the true owner or controlling interests of the entity;
- requests for undue levels of secrecy or unwillingness to give the names of its real owners and controllers;
- is incorporated, has its principal place of business or carries a larger part of its activities in a jurisdiction that Botswana, or the Authority, has blacklisted;
- is subject to international sanctions or other economic measures.

2.1.3 Certification Policy and Certification Practice Statement

2.1.3.1 The CA must draw up a **Certification Policy** (**CP**) detailing what the certificate can be used for, as well as a **Certification Practice**

Statement (**CPS**), comprehensively describing the CA's internal practices and operating procedures, tasks and responsibilities within the organization. The implications of the Certificate Policy and Certification Practice Statement must be brought to the attention of all relevant parties.

2.1.3.2 When drawing up the CP and CPS, a CA is to comply with all the objectives, requirements and procedures found in **Sections 5.6, 5.7, 5.8, 6, 7.2.1** and **8.2.1** of **ISO 21188: 2006.** Additionally:

2.1.3.2.1 Wherever a change in the CP or CPS has been approved by BOCRA, a copy of the latest version of the CP and the CPS (or alternatively, of a PKI Disclosure Statement, if the CPS is not published), together with its effective date, must be published on the CA's website in a prominent manner as required by **Regulation 11(3).** A version number must also be provided.

2.1.3.2.2 Prior notice of intended changes must be given to all relevant parties at least one (1) month before such changes are effected.

2.1.4 Subscriber/Subject Protection, Terms & Conditions

2.1.4.1 In addition to drawing up the CP and CPS, the CA must also draw up the terms and conditions regarding the use of the certificate that must be made available to all relevant parties and must be presented to BOCRA upon application for accreditation. These must include:

- the qualified certificate policy being applied and any limitations on its use;
- all subscriber obligations,
- easily accessible policies and procedures for the resolution of complaints and disputes received from customers in relation to its services;

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

- details on validation of the certificate, including requirements to check the revocation status of the certificate;
- limitations of liability being accepted by the CA, including the purposes/uses for which the CA accepts (or excludes) liability;
- consent to the keeping of records of information used in registration and the period of time for which registration information is retained by the CA;
- the type of events logged and the period of time for which they are retained;
- device provision and any subsequent revocation;
- identity and any specific attributes of the subject placed in the certificate;
- the manner in which information is passed on to third parties in the event of the CA terminating its services;
- whether, and under what conditions, the subscriber consents to the publication of the certificate; and
- Confirmation that the information held in the certificate is correct.

2.1.4.2 Certificates must be available for retrieval only in those cases for which the subject's consent has been obtained.

2.1.4.3 The terms and conditions must be in a durable form and in easily understandable language. The CA shall record the signed agreement with the subscriber and the information identified above must be retained for the period of time indicated to the subscriber and as detailed in **Part 2.2.10.**

2.1.4.4 Information contained in a certificate and the terms and conditions of its use must be publicly and internationally available 24 hours per day, 7 days per week. A system failure must be rectified within the time period stated in CPS.

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

2.2 CA Environmental Controls

2.2.1 Security Management

2.2.1.1 The CA shall ensure that administrative and management procedures are applied to ensure that security is adequate and corresponds to recognized standards in relation to the certification services it is providing. Thus, the CA must comply with all the objectives, requirements and procedures found in **Sections 7.2.2** and **8.2.2** of **ISO 21188: 2006.** Additionally:

2.2.1.1.1 Any changes that will impact significantly the level of security provided must be approved by BOCRA in accordance with **Regulation 11**.

2.2.2 Asset Classification and Management

2.2.2.1 A CA must maintain an inventory of all information assets, assign a classification for the protection requirements to those assets (after conducting the necessary risk analysis) and must ensure that such assets and information are adequately protected. Thus, the CA must ensure comply with all the objectives, requirements and procedures found in **Sections 7.2.3** and **8.2.3** of **ISO 21188: 2006.**

2.2.3 Personnel

2.2.3.1 A CA must ensure that its personnel are fit and proper persons in possession of the the relevant expert knowledge, experience, and qualifications in relation to their particular job function, as required by **Schedule 5 of the Regulations**. The CA must also have in place measures to control access of personnel to sensitive information and functions.

2.2.3.2 "Expert knowledge, experience and qualifications" should be understood as meaning that formal training and credentials, actual experience, or a combination of the two are required. Additionally, personnel must possess knowledge of the Act, the Regulations and these ACS Standards.

2.2.3.3 Additionally, all CA **Trusted Personnel** must be free from conflicting interests that might prejudice the impartiality of the CA operations. Senior executives, senior staff and staff in trusted roles, must be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides. There must be a documented structure which safeguards impartiality of operations.

2.2.3.4 The CA shall ensure that personnel shall be held accountable for their activities, for example through the retention and review of event logs.

2.2.3.5 As required by **Schedule 2 of the Regulations,** the CA shall not employ persons that have been convicted, whether in Botswana or elsewhere, of an offence the conviction for which involved a finding **of fraud or dishonest behaviour,** or an offence under the Act or the Regulations**.**

2.2.3.6 The CA must also be compliant with **Sections 7.2.4** and **8.2.4 of ISO 21188: 2006.**

2.2.4 Physical and Environmental Security

2.2.4.1 The CA must ensure that physical access to critical services is controlled and physical risks to its assets minimized. Thus, the CA must ensure that it complies at all times with the requirements found in **Sections 7.2.5** and **8.2.5 of ISO 21188: 2006.** It should

also ensure that persons entering a physically secure area shall not be left for any significant period without oversight by senior management.

2.2.5 Operations Management

2.2.5.1 CA systems must be operated securely, with minimal risk of failure. In order to ensure this, the CA must ensure that it complies with **Sections 7.2.6** and **8.2.6 of ISO 21188.** Additionally:

2.2.5.1.1 Media management procedures must protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

2.2.5.1.2 Capacity demands must be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

2.2.6 System Access Management

2.2.6.1 The CA must ensure that its system access is limited to properly authorized individuals**.** In order to ensure this, the CA must ensure that it complies with **Sections 7.2.7** and **8.2.7 of ISO 21188.** Additionally:

2.2.6.1.1 Sensitive data must not be accessible by unauthorized users through re-used storage objects (e.g. deleted files).

2.2.6.1.2 Continuous monitoring and alarm facilities must be provided to enable the CA to immediately detect any unauthorized and/or irregular attempts to access its resources.

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

2.2.6.1.3 Access control shall be enforced on addition or deletion of certificate attempts, as well as on modification attempts of certificates and other associated information, including certificate metadata.

2.2.6.1.4 Access control shall be enforced on revocation status modification attempts and attempts at modifying any related information.

2.2.7 Systems Development and Maintenance

2.2.7.1 The CA shall use trustworthy systems and products that are protected against unauthorized modification, in order to maintain system integrity at all times**.** Thus, the CA must ensure that it complies with **Sections 7.2.8** and **8.2.8** of **ISO 21188**.

2.2.8 Business Continuity

2.2.8.1 The CA must implement an incident management plan to provide for security breaches and other operational difficulties which may arise, and must immediately report the occurrence of any such events to the BOCRA and to the relevant parties. The CA must ensure that it complies with **Sections 7.2.9** and **8.2.9 of ISO 21188.** Additionally:

2.2.8.1.1 The incident management plan shall, as a minimum, provide for the:

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

- compromise of a key including compromise or suspected compromise of a CA's private signing key;
- unauthorized access to the certification service provider's systems;
- unavailability of the infrastructure; and
- Fraudulent registration and generation of certificates, certificate suspension and revocation information.

2.2.8.1.2 The following measures are put into place in the incident management plan:

- Dual control should be applied to recovery where possible.

- When a CA is informed of the compromise of another CA, any certificate that has been issued for the compromised CA is to be revoked.

- Should any of the algorithms, or associated parameters, used by the CA or its subscribers become insufficient for its remaining intended usage then the CA shall inform all relevant parties with which the CA has an established relationship. In addition, this information shall be made available to other relying parties and any affected certificate shall be revoked.

2.2.8.2 Where an incident has been reported to BOCRA in accordance with this part, BOCRA may mandate that certain actions be taken by the CA with immediate effect. Such actions may include public disclosure of the incident, if BOCRA deems that this measure is critical to the general public.

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

2.2.9 Monitoring and Compliance

2.2.9.1 The CA must implement controls to ensure that it conforms to the relevant legal, regulatory and contractual requirements, as well as to its own security policies and procedures. Thus, the CA must ensure that it complies with **Sections 7.2.10** and **8.2.10 of ISO 21188.**

2.2.10 Audit Logs

2.2.10.1 The CA must ensure that all relevant information concerning a qualifying certificate is recorded in a manner so as to provide evidence of certification in legal proceedings, if required.

2.2.10.2 Accordingly, the CA must comply with all the objectives, requirements and procedures found in **Sections 7.2.11 and 8.2.11** of **ISO 21188.** Additionally:

2.2.10.2.1 The CA must detail the information which it records and the manner in which this is done, in its CP, CPS and Terms and Conditions, so that signatories and relying parties are fully aware of any limitations.

2.2.10.2.2 Records should be kept for a period of ten (10) years, unless the CA can obtain a waiver of this requirement from BOCRA**,** due to the fact that the circumstances for which its services are used do not require retention for this period.

2.2.10.2.3 The CA should state within its practices the clock used in timing of events, and how accuracy is ensured.

2.3 CA Key Life Cycle Management Controls

2.3.1 CA Key Generation

2.3.1.1 The CA must ensure that key pairs are generated securely as detailed in the CPS. Accordingly, the CA must comply with the requirements and procedures found in **Sections 7.3.1 and 8.3.1** of **ISO 21188.** Additionally:

2.3.1.1.1 At least three (3) months before expiration of its CA signing key, the CA must generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key is to be generated and distributed in accordance with this document.

2.3.2 CA Key Storage, Backup and Recovery

2.3.2.1 The CA must ensure confidentiality and integrity of CA private keys and that access to the CA's cryptographic hardware is limited to authorized individuals. Accordingly, the CA must comply with the requirements and procedures found in **Sections 7.3.2 and 8.3.2** of **ISO 21188.** Additionally:

2.3.2.1.1 The CA private signing key must be subject to the same level of protection as provided by the secure cryptographic device at all times.

2.3.2.1.2 The CA private signing key is to be backed up, stored and recovered only by Trusted Personnel using, at least, dual control while keeping number of personnel authorised to carry out this function to a minimum.

2.3.3 CA Key Distribution

2.3.3.1 The CA must ensure that the integrity and authenticity of the CA signature verification (public) key and any associated parameters are maintained during its distribution to relying parties. Accordingly, the CA must comply with the requirements and procedures found in **Sections 7.3.3 and 8.3.3** of **ISO 21188.**

2.3.4 Key Usage

2.3.4.1 The CA must ensure that its private signing keys are not used inappropriately and thus it must comply with the requirements and procedures found in **Sections 7.3.4 and 8.3.4** of **ISO 21188.**

2.3.4.2 CA signing key(s) used for generating certificates may also be used to sign other types of certificates and revocation status information, as long as operational requirements for the CA environment are upheld and the certificate signing keys are only used within physically secure premises.

2.3.5 CA Key Archival and Destruction

2.3.5.1 The CA must ensure that archived CA keys remain confidential and secured in the event that they are put back into production and that CA keys are completely destroyed at the end of the key pair life cycle as determined by the CPS. Accordingly, it must comply with the requirements and procedures found in **Sections 7.3.5 and 8.3.5** of **ISO 21188.**

2.3.6 CA Key Compromise

2.3.6.1 The CA must ensure that continuity of operations is maintained to the maximum extent possible in the event of the compromise of the CA's private keys. Accordingly, it must comply with the

requirements and procedures found in **Sections 7.3.6 and 8.3.6** of **ISO 21188.**

2.4 Subject Key Life Cycle Management Controls

2.4.1 CA-provided Subject Key Generation Services

2.4.1.1 The CA must ensure that signatory keys are generated securely in accordance with the CP and that the secrecy of the private key is guaranteed at all times, including during distribution. Accordingly, it must comply with the requirements and procedures found in **Sections 7.4.1** and **8.4.1** of **ISO 21188.** Additionally:

2.4.1.1.1 Signatory keys generated by the CA must be stored securely before delivery to the subject and must be delivered in a manner such that the secrecy and the integrity of the key is not compromised. Once delivered to the subject, any copies of the subject's private key held by the CA must be destroyed.

2.4.1.1.2 The subject must be able to keep the private key under his sole control at all times.

2.4.2 CA -provided Subject Key Storage and Recovery Services

2.4.2.1 Where the CA provides subject confidentiality key storage, recovery or escrow services, it shall ensure that subject private keys stored, archived or in escrow by the CA remain secure and confidential at all times and that subject private keys stored by the CA are completely destroyed at the end of the key pair life cycle. Accordingly, it must comply with the requirements and procedures found in **Sections 7.4.2** and **8.4.2** of **ISO 21188.**

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

2.4.3 Integrated Circuit Card (ICC) Life Cycle Management

2.4.3.1 Where the CA distributes subject key pairs and certificates using integrated circuit cards (ICCs), it shall ensure that ICC procurement, preparation and personalization are securely controlled by it or any sub-contracted parties and usage is enabled prior to ICC issuance. Furthermore, ICCs must be securely stored, distributed and replaced, and that ICCs returned to the CA are securely terminated. Accordingly, it must comply with the requirements and procedures found in **Sections 7.4.3** and **8.4.3** of **ISO 21188.**

2.4.4 Requirements for Subject Key Management

2.4.4.1 The CA must prescribe the means to securely manage subject keys throughout the key life cycle. In doing so, it must comply with **Sections 7.4.4** and **8.4.4** of **ISO 21188: 2006.**

2.4.5 Secure-signature-creation device preparation

2.4.5.1 The CA must ensure the integrity of a SSCD that the process is carried out securely this includes the verification of integrity before each use. As a minimum, this means that in addition to ISO 21188, the CA must abide by the following principle:

2.4.5.1.1 Secure-signature-creation device preparation shall be securely controlled by the CA by using a suitable protection profile, defined in accordance with **ISO/IEC 15408** or equivalent;

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

2.5 Certificate Management Requirements

2.5.1 Subject Registration

2.5.1.1 Since the CA is liable for the accuracy of the information contained in a certificate issued by it, it must have detailed procedures in place for subject registration to ensure that subjects are properly identified. Furthermore, it must ensure that any certificate requests are accurate, authorized and complete. Accordingly, it must comply with **Sections 7.5.1** and **8.5.1** of **ISO 21188: 2006.**

2.5.1.2 Where the subject is an individual obtaining the certificate **for his/her individual use**, evidence must be provided to the CA of:

- name of the subject (including surname and given names);
- date and place of birth of the subject;
- passport/identity card number or other unique identification data relating to the subject, allowing him/her to be distinguished from other individuals with the same or a similar name;
- a physical address and other details where the subject may be contacted.

Official identification documents used for the purposes of this section must be **valid and not expired.**

2.5.1.3 Where the subject is obtaining the signature **on behalf or in association with an entity**, evidence of the following must also be provided to the CA:

BOTSWANA COMMUNICATIONS REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

- full name and legal status of the entity;
- registration information of the entity;
- Evidence that the subject is associated with the entity and has the authority to act on its behalf.

2.5.1.4 Further to receipt of the evidence above, the CA must, before completing registration, verify:

- by appropriate means, the authenticity of the evidence provided in accordance with Paragraph 2.5.1.2 and 2.5.1.3 above;
- the identity of the subject (and subscriber, where applicable) as detailed in the same Paragraphs 2.5.1.2 and 2.5.1.3;
- the uniqueness of the subject's name as appearing on the certificate;
- that the subject/subscriber is fully aware of the terms and conditions in the CA's terms and conditions the CP and the CPS;
- That any a domain name contained in the certificate can be rightfully used by the subject/subscriber.

2.5.1.5 Evidence of the identity of an individual should be checked against a physical person directly. Where this is not possible, means which provide equivalent assurance to physical presence should be used. By way of illustration, the subject can provide a certified copy of his identification documents together with a declaration that the said documents correspond to the image and likeness of the subject. Certification and declaration must be carried out by a legal professional, accountancy professional, notary or equivalent. In all cases of such 'indirect verification', the CA must carry out additional checks on both subject and certifier. Recognised commercial electronic data providers may be useful for such purposes.

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

2.5.2 Certificate Renewal, Re-Key & Update

2.5.2.1 The CA must ensure that certificate renewal, re-key and update requests, where supported, are complete, accurate and duly authorized. Accordingly, it must comply with **Sections 7.5.2, 8.5.2, 7.5.3 and 8.5.3** of **ISO 21188: 2006.** Additionally:

2.5.2.1.1 Before renewal, re-key or update a CA must:

- verify the identity of the requesting party;
- confirm that the information and evidence presented during the initial registration of the subject, as identified in Paragraphs 2.5.1.2 and 2.5.1.3, is still valid;
- obtain updated versions of any expired identification documents;
- repeat identify verification procedures detailed in the Part 2.5.1 if the distinguished name or any significant information has changed from the initial registration;
- verify that the subject/subscriber is fully aware of any changes in the CA's terms and conditions, the CP and the CPS;
- verify that any a domain name contained in the certificate can still be rightfully used by the subject/subscriber;
- Verify that the subject is associated with an entity still has the authority to act on its behalf.

2.5.2.1.2 The CA should notify subscribers of the need for renewal and re-key two (2) months before its expiry.

2.5.2.1.3 The start date of the renewed certificate must be the same as that in the original certificate.

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

2.5.3 Certificate Issuance

2.5.3.1 The CA must ensure that it generates and issues certificates securely, as detailed in its CP and CPS, to maintain their authenticity and integrity. Accordingly, it must comply with **Sections 7.5.4 and 8.5.4** of **ISO 21188: 2006.** Additionally:

2.5.3.1.1 The CA cannot re-assign a specific distinguishable name which has been used in an issued certificate to another subject or subscriber.

2.5.4 Certificate Distribution

2.5.4.1 The CA must ensure that certificates are made available as necessary to subscribers, subject persons and relying parties through a secure communication channel, established to ensure the authenticity, integrity and confidentiality of the exchanges. Accordingly, it must comply with **Sections 7.5.5** and **8.5.5** of **ISO 21188: 2006.**

2.5.5 Certificate Revocation

2.5.5.1 The CA must ensure that certificates are revoked in a timely manner as required in the circumstances of the case and based on authorized and validated certificate revocation requests. In doing so, the CA must comply with **Sections 7.5.6** and **8.5.6** of **ISO 21188: 2006.** Additionally:

2.5.5.1.1 The time between the receipt of a request or report and the change to revocation status information being available to all relying parties **shall never exceed one (1) day**. A certificate's revocation status may be set to 'suspended' while the revocation is being confirmed.

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

2.5.5.1.2 The CA is to provide a means of rapid communication for certificate revocation services as detailed in the CP and CPS, and which must be available **24 hours per day, 7 days per week**. Revocation status information shall be publicly and internationally available and shall continue to include information on the status of a certificate at least until the certificate expires.

2.5.5.1.3 The CA should detail the maximum length of time for which a certificate can remain suspended before it is definitively revoked.

2.5.6 Certificate Suspension

2.5.6.1 Where certificate suspension is supported, the CA must ensure that certificates are suspended in a timely manner, as required in the circumstances of the case and based on authorized and validated certificate suspension requests. The CA must comply with **Sections 7.5.7** and **8.5.7** of **ISO 21188: 2006.**

2.5.7 Certificate Validation Services

2.5.7.1 The CA shall maintain controls to provide reasonable assurance that timely, complete and accurate certificate status information (including certificate revocation lists and other certificate status mechanisms) is made available to relevant parties in accordance with the CP. In doing so, the CA must comply with **Sections 7.5.8** and **8.5.8** of **ISO 21188: 2006.**

2.6 CA Certificate Life Cycle Management Controls

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw

2.6.1 Subordinate CA Certificate Life Cycle Management

2.6.1.1 A parent CA shall maintain all the necessary controls to ensure the security and integrity of subordinate CA certificates. Accordingly, it must comply with **Sections 7.6.1** and **8.6.1** of **ISO 21188: 2006.**

BOTSWANA COMMUNICATIONS
REGULATORY AUTHORITY
PLOT 206/207 INDEPENDENCE AVENUE
PRIVATE BAG 00495 , GABORONE, BOTSWANA
TEL: +267 3957755 FAX: +267 3957976
info@bocra.org.bw I www.bocra.org.bw