Accredited Certification Standards

Compliance Checklist

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 awarded in accordance with the Regulations;
"Act"	means the Electronic Communication and Transactions Act.
"All relevant parties"	means subscribers, subjects and relying parties;
"Auditor"	means a team of auditors as detailed in **Regulation 6 of the Regulations**;
"BOCRA"	means the Botswana Communications Regulatory Authority;
"Certification Practice Statement"	means a statement issued by a certification service provider, specifying the practices that it exercises in issuing certificates.
"Certification Authority" or CA	means Secure Electronic Signature Providers accredited in accordance with Section 25 of the Act and the **Regulations**;
"ETSI"	means the European Telecommunications Standards Institute.
"ETSI TS 101 456"	means the "Policy requirements for certification authorities issuing qualified certificates" issued by ETSI.
"ISO"	means the International Organisation for Standardization.
"ISO21188:2006"	means International Standard (Public key infrastructure for financial services - Practices and policy framework) issued by ISO.
"Qualifying certificate"	means a certificate which conforms with the requirements of **Schedule 3 of the Regulations** in the manner detailed in these ACS Standards.
"Qualifying signature creation device" or QSCD	means a signature creation device which conforms with the requirements of **Schedule 2 of the Regulations** in the manner detailed in these ACS Standards.

"Regulations"	means the Electronic Communications and Transactions Regulations.
"Signatory"	means a person who holds a signature creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents.
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 service provider.
"the ACS Checklist"	means the current document, namely the Accredited Certification Standards Compliance Checklist published by the Communications Regulatory Authority for compliance audit purposes;
"the ACS Standards"	means the Accredited Certification Service Standards published by the Authority in accordance with **Regulation 4(2).**
"the Authority"	means BOCRA.
"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.
"Web Trust"	means the document entitled "Trust Service Principles and Criteria for Certification Authorities" Version 2.0 drafted by the Canadian Institute of Chartered Accountants.

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. Preliminary Note

This **Accredited Certification Standards Compliance Checklist** ("**ACS Checklist**") is to be completed by an Auditor in relation to a Certification Authority (CA) whenever BOCRA so requests, in accordance with the relevant provisions of the Regulations.

The ACS Checklist reflects the current version of the ACS Standards, which have been issued in accordance with **Regulation 4(2)** 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 the ACS Standards.

The ACS Standards require a 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). This is the standard which many national standards around the are based on. In order to cater, as much as possible, for interoperability with the European Union, a few requirements have been mandated additionally, to address some requirements imposed by **ETSI TS 101 456,** the "Policy requirements for certification authorities issuing qualified certificates" issued by ETSI**. 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 additional requirements provided as detailed below**. This does not mean that the service provider needs to be certified as compliant by ISO; however the obtainment of such certification will mean that only the additional provisions in this document will need to be audited in accordance with **Regulation 6,** unless some form of exemption has been obtained from BOCRA.

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

It should be noted that since the audit report can occur at the stage of application for accreditation, as well as during operations of an accredited certification service provider and before renewal of such accreditation, this ACS Compliance Checklist provides for situations where operations have not yet commenced, as well as situations where operations have already been ongoing. Thus, the phrases “complies/is able to comply”, and “are being/shall be (as applicable)” (as well as similar phrases) are to be interpreted in this light (i.e. “is able to comply” and “shall be” refer **only to situations where this checklist is being compiled at the stage of the initial application for accreditation**).

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. Mandatory Requirements for CA's – Report Outline

Requirements	***Yes/ No***	***Checks carried out***	***Comments***
General Requirements (ACS Part 2.1)			
Overarching Principles			
The Auditor shall verify that the CAs policies show its intention to: 1. Operate in a manner that is fair, just and non-discriminatory. 2. Make its services accessible to any applicant who requests them in the absence of a valid reason. 3. Operate in compliance with data protection legislation in Botswana when processing and storing information during the provision of its services. 4. Comply with the ACS Standards, the Act and Regulations. The CA's policies, terms and conditions are transparent and publically available, and they state that prior notice of intended changes will be given to all relevant			

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

parties at least one (1) month before such changes are effected. The Auditor shall ensure that where the CA has outsourced parts of its procedures, detailed agreements are in place with all subcontractors. Where the CA is already accredited, the Auditor shall investigate whether the CA is operating in accordance with the principles outlined above.			
Fit & Proper Persons			
Where the CA is already accredited, the Auditor shall check whether there has been any change in the ownership of the body corporate. (Other fit & proper tests are generally carried out by BOCRA).			
Certification Policy (CP) and Certification Practice Statement (CPS)			
The Auditor shall verify that: 1. The CA's Certification Policy and Certification Practice Statement comply with **Sections 5.6, 5.7, 5.8, 6, 7.2.1** and **8.2.1** 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

2. Where the CA is already accredited, a copy of the latest version of the CP and the CPS (or alternatively, of a PKI Disclosure Statement together with its effective date, is published on the CA's website in a prominent manner. 3. Where the CA is already accredited, prior notice of intended changes was generally given to all relevant parties at least one (1) month before such changes were effected. 4. Where the CA has outsourced parts of its procedures, details of the subcontractors' policies and practices are clarified in the CA's Certification Policy and Certification Practice Statement.			
Subscriber/Subject Protection, Terms & Conditions			
The Auditor shall verify that: 1. The CA has drawn up the Terms and Conditions of the use of the certificate and these contain the following: • 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; • 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;			

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

• confirmation that the information held in the certificate is correct. 2. The Terms and Conditions are and have been (where applicable) available in a durable form and in easily understandable language. 3. Certificates are and have been (where applicable) available for retrieval only in those cases for which the subject's consent is/has been obtained. 4. The said terms and conditions are to are and have been (where applicable) made public at all times. 5. The CA shall record/has recorded (as applicable) the signed agreements with subscribers. 6. Information contained in the subscriber agreement will be/has been (as applicable) retained for a period of time as indicated to the subscriber in the same terms and conditions/CPS and as detailed in **Part 0 of the ACS Standards**. 7. Information contained in a certificate and the terms and			

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

conditions of its use shall be/has been (as applicable) publicly and internationally available 24 hours per day, 7 days per week. 8. A process is in place to ensure that system failures shall be rectified within the time period stated in the terms and conditions/CPS. 9. Where the CA is accredited, system failures were rectified within the time period stated in the terms and conditions/CPS.			
Environmental Controls (ACS Part 2.2)			
Security Management			
The Auditor shall verify that: 1. The CA complies/is able to comply with **Sections 7.2.2 and 8.2.2 of ISO 21188: 2006.** 2. Where the CA is accredited, any changes in the CA's operation (from the time of its accreditation) that significantly impacted the level of security provided, were approved by BOCRA in accordance with **Regulation 10.**			
Asset Classification and Management			

The Auditor shall verify that the CA complies/is able to comply with **Sections 7.2.3** and **8.2.3** of **ISO 21188: 2006.**			
Personnel			
The Auditor shall review all employment policies. The Auditor shall carry out checks on CA's current or proposed Trusted Personnel to ensure that: 1. They have not 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. They have formal training and credentials, actual experience, or a combination of the two. 3. Senior executives, senior staff and staff in trusted roles, are free from any commercial, financial and other pressures which might adversely influence trust in the services it provides. The Auditor shall furthermore ensure that:			

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. The CA keeps a documented structure which safeguards impartiality of operations. 2. The CA has policies and procedures in place to ensure that all personnel shall be held accountable for their activities. 3. The CA is compliant/is able to comply with **Sections 7.2.4 and 8.2.4 of ISO 21188: 2006.**			
Physical and Environmental Security			
The Auditor shall verify that the CA: **1.** Complies/is able to comply at all times with the requirements found in **Sections 7.2.5 and 8.2.5 of ISO 21188: 2006.** 2. The CA employs a policy whereby persons entering a physically secure area shall not be left for any significant period without oversight by senior management.			
Operations Management			
The Auditor shall verify that the CA: 1. Complies/is able to comply with Sections 7.2.6 and 8.2.6 of ISO 21188.			

2. Media management procedures protect against obsolescence and deterioration of media within the period of time that records are required to be retained. 3. Capacity demands are/shall be (as applicable) monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.			
System Access Management			
The Auditor shall verify that the CA: 1. Complies/is able to comply with **Sections 7.2.7 and 8.2.7 of ISO 21188.** 2. Has systems in place to ensure that sensitive data is not accessible by unauthorized users through re-used storage objects (e.g. deleted files). 3. Continuous monitoring and alarm facilities are in place to enable the CA to immediately detect any unauthorized and/or irregular attempts to access its resources. 4. Access control is/shall be enforced on addition or deletion			

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

of certificate attempts, as well as on modification attempts of certificates and other associated information, including certificate metadata. 5. Access control is/shall be enforced on revocation status modification attempts and attempts at modifying any related information.			
Systems Development and Maintenance			
The Auditor shall verify that the CA complies/is able to comply with **Sections 7.2.8 and 8.2.8 of ISO 21188.**			
Business Continuity			
The Auditor shall verify whether: 1. The CA has implemented an incident management plan to provide for security breaches and other operational difficulties which may arise. 2. The incident management plan provides for the following: • The compromise of a key including compromise or suspected compromise of a CA's private signing key;			

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

• The unauthorized access to the certification service provider's systems; • The unavailability of the infrastructure; • Fraudulent registration and generation of certificates, certificate suspension and revocation information. • Dual control should to 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. • Where 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. 3. The CA's policies provide that security breaches and other operational difficulties will be immediately reported to BOCRA and to the relevant parties.			

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

4. Where the CA is already accredited, any security breaches and other operational difficulties which occurred were immediately reported to BOCRA and to the relevant parties. 5. The CA complies/is able to comply with **Sections 7.2.9** and **8.2.9 of ISO 21188.** 6. Where an incident was reported to BOCRA the CA carried out any orders given by BOCRA with immediate effect.			
Monitoring and Compliance			
The Auditor shall verify that the CA complies/is able to comply with **Sections 7.2.10 and 8.2.10 of ISO 21188.**			
Audit Logs			
The Auditor shall verify that the CA: 1. Complies/is able to comply with all the objectives, requirements and procedures found in **Sections 7.2.11 and 8.2.11** of **ISO 21188.** 2. Has detailed the information which it records/shall be recording (as applicable) and the manner in which this is done/shall be done, in its CP,			

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

CPS and Terms and Conditions, so that signatories and relying parties are fully aware of any limitations. 3. Records are being/shall be (as applicable) kept for a period of ten (10) years, unless the CA has obtained a waiver of this requirement from BOCRA**.** 4. The CA has stated within its practices the clock used in timing of events, and how accuracy is ensured.			
CA Key Life Cycle Management Controls (ACS Part 2.3)			
CA Key Generation			
The Auditor shall verify that: 1. The CA complies/is able to comply with the requirements and procedures found in **Sections 7.3.1 and 8.3.1** of **ISO 21188.** 2. The CAs policies provide that 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.			

3. Where the CA is already accredited, it has abided by the three (3) month period detailed above and other principles detailed above. 4. Where the CA is already accredited, the new CA keys were generated and distributed in accordance with the ACS Standards.			
CA Key Storage, Backup and Recovery			
The Auditor shall verify that: 1. The CA complies/is able to comply with the requirements and procedures found in **Sections 7.3.2 and 8.3.2** of **ISO 21188.** 2. The CA private signing key is subject to the same level of protection provided by the secure cryptographic device at all times. 3. The CA private signing key is to be backed up, stored and recovered only by Trusted Personnel using, at least, dual control.			
Key Usage			

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

The Auditor shall verify that: 1. The CA complies/is able to comply with the requirements and procedures found in **Sections 7.3.4 and 8.3.4** of **ISO 21188.** 2. Where CA signing key(s) are also used to sign other types of certificates and revocation status information, the same operational requirements for the CA environment are upheld and the certificate signing keys are only used within physically secure premises.			
CA Key Archival and Destruction			
The Auditor shall verify that the CA complies/is able to comply with the requirements and procedures found in **Sections 7.3.5 and 8.3.5** of **ISO 21188.**			
CA Key Compromise			
The Auditor shall verify that the CA complies/is able to comply with the requirements and procedures found in **Sections 7.3.6 and 8.3.6** of **ISO 21188.**			
Subject Key Life Cycle Management Controls (ACS Part 2.4)			
CA-provided Subject Key Generation Services			

The Auditor shall verify that: 1. The CA complies/is able to comply with the requirements and procedures found in **7.4.1** and **8.4.1** of **ISO 21188.** 2. The CA has a system to ensure that signatory keys generated by the CA are stored securely before delivery to the subject and are delivered in a manner such that the secrecy and the integrity of the key is not compromised. 3. Once delivered to the subject, any copies of the subject's private key held by the CA are destroyed. 4. The subject is able to keep the private key under his sole control at all times.			
CA - provided Subject Key Storage and Recovery Services			
The Auditor shall verify that the CA complies/is able to comply with the requirements and procedures found in **Sections 7.4.2** and **8.4.2** of **ISO 21188.**			
Integrated Circuit Card (ICC) Life Cycle Management			
The Auditor shall verify that the CA complies/is able to comply with the			

requirements and procedures found in **Sections 7.4.3** and **8.4.3** of **ISO 21188.**			
Requirements for Subject Key Management			
The Auditor shall verify that the CA complies/is able to comply with **Sections 7.4.4** and **8.4.4** of **ISO 21188: 2006.**			
Secure-signature-creation device preparation			
The Auditor shall verify that secure-signature-creation device preparation is securely controlled by the CA by using a suitable protection profile, defined in accordance with **ISO/IEC 15408** or equivalent.			
Certificate Management Requirements (ACS Part 2.5)			
Subject Registration			
The Auditor shall verify that: 1. The CA complies/is able to comply with **Sections 7.5.1** and **8.5.1** of **ISO 21188: 2006.** 2. The CA's subject registration process complies with the requirements detailed in **Paragraphs 2.5.1.2 to 2.5.1.5 of the ACS Standards.**			

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

Certificate Renewal, Re-Key & Update			
The Auditor shall check whether: 1. The CA complies/is able to comply with **Sections 7.5.2, 8.5.2, 7.5.3 and 8.5.3** of **ISO 21188: 2006.** 2. The CA's registration process for renewal, re-key or update complies with the requirements detailed in **Paragraph 2.5.2.1.1 of the ACS Standards.** 3. Where the CA is already accredited it has been notifying subscribers of the need for renewal and re-key two (2) months before its expiry.			
Certificate Issuance			
The Auditor shall verify that: 1. The CA complies/is able to comply with **Sections 7.5.4 and 8.5.4** of **ISO 21188: 2006.** 2. The CAs policies provide that a specific distinguishable name which has been used in an issued certificate to another subject or subscriber is not re-assigned. 3. Where the CA is already accredited it has conformed with the abovementioned policy			

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

regarding distinguishable names.			
Certificate Distribution			
The Auditor shall verify that the CA complies/is able to comply with **Sections 7.5.5** and **8.5.5** of **ISO 21188: 2006.**			
Certificate Revocation			
The Auditor shall verify that: 1. The CA complies/is able to comply with **Sections 7.5.6** and **8.5.6** of **ISO 21188: 2006.** Additionally: 2. The CAs policies provide that 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**. 3. The CAs policies detail the maximum length of time for which a certificate can remain suspended before it is definitively revoked.			

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

4. Where the CA is already accredited it has conformed with the abovementioned policy regarding timing for effecting a revocation request. 5. The CA provides a means of rapid communication for certificate revocation services as detailed in the CP and CPS, and which is available **24 hours per day, 7 days per week**. 6. The CA provides/shall provide (as applicable) revocation publicly and internationally available status information of a certificate at least until the certificate expires.			
Certificate Suspension			
Where certificate suspension is supported, the Auditor shall verify that the CA complies/is able to comply with **Sections 7.5.7** and **8.5.7** of **ISO 21188: 2006.**			
Certificate Validation Services			
The Auditor shall verify that the CA complies/is able to comply with			

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

Sections 7.5.8 and 8.5.8 of ISO 21188: 2006.			
CA Certificate Life Cycle Management Controls			
Subordinate CA Certificate Life Cycle Management			
The Auditor shall verify that a parent CA complies/is able to 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