NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA)

PUBLIC KEY INFRASTRUCTURE (PKI) REGULATIONS

Code of Practice for Accredited Certificate Authorities (CAs)

Table of Contents

Change Management History

Change Number	Revision Description	Reviewer	Pages Affected	Revision Number	Date (MM/YYY
0	None	Inye Kemabota	0	0	September 2014

AUTHORITY

In the exercise of the powers conferred on it by section 6 of the National Information Technology Development Agency Act of 2007 (under the auspices of the Federal Ministry of Communication Technology), NITDA hereby issues the following regulation on Public Key Infrastructure.(PKI)

DEFINITION OF TERMS

The terms used in this Code of Practice are defined as follows:

Certificate

Means a record which

(a) is issued by a CA for the purpose of supporting a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;

(b) identifies the CA issuing it;

(c) names or identifies the person to whom it is issued;

(d) contains the public key of the person to whom it is issued;

(e) is signed by the CA issuing it

Certification Authority or CA

Means - a person who issues a certificate to a person (who may be another CA)

Certification Authority Certificate or CA Certificate

Means - a certificate issued by or to a CA for the purpose of certifying certificates issued by that CA. This certificate may be issued by a CA for its own use or by one CA to another CA

Certification Authority Disclosure Record

In relation to a recognized CA, means the record maintained under section 31 of the Ordinance for that recognized CA

Certificate Policy or CP

Means a named set of rules that indicates the applicability of a certificate to a particular community and/or class of usage with common security requirements

Certification Practice Statement or CPS

Means a statement issued by a recognized CA to specify the practices and standards that the recognized CA employs in issuing certificates

Certificate Revocation List or CRL

Means a list maintained and published by a certification authority to specify the certificates that are issued by it and that have been revoked.

Digital Signature

In relation to an electronic record, means an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine

(a) whether the transformation was generated using the private key that corresponds to the signer's public key;

(b) whether the initial electronic record has been altered since the transformation was generated

Electronic Record

Means a record generated in digital form by an information system, which can be

(a) transmitted within an information system or from one information system to another;

(b) stored in an information system or other medium

Information

Includes data, text, images, sound codes, computer programmes, software and databases;

Information System

Means a system which

(a) processes information;

(b) records information;

(c) can be used to cause information to be recorded, stored or otherwise processed in other information systems (wherever situated); and

(d) can be used to retrieve information, whether the information is recorded or stored in the system itself or in other information systems (wherever situated);

Issue

In relation to a certificate, means to—

(*a*) create the certificate, and then notify the person named or identified in the certificate as the person to whom the certificate is issued of the information on the person as contained in the certificate; or

(*b*) notify the person to be named or identified in the certificate as the person to whom the certificate is issued of the information on the person that is to be contained in the certificate, and then create the certificate, and then make the certificate available for use by the person;

Key Pair

In an asymmetric cryptosystem, means a private key and its mathematically related public key, where the public key can verify a digital signature that the private key generates.

Properly Authorised Person

Means a person who is authorised to act for the subscriber

Private Key

Means the key of a key pair used to generate a digital signature

Public Key

Means the key of a key pair used to verify a digital signature

Recognized Certificate

(a) a certificate recognized by the Controller
(b) a certificate of a type, class or description of certificate recognized by the Controller
(c) a certificate designated as a recognized certificate and issued by the Controller.

Recognized Certification Authority or Recognized CA

Means a CA recognized under section 21 of the Ordinance or the Postmaster General

Record

Means information that is inscribed on, stored in or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in a perceivable form.

Repository

Means an information system for storing and retrieving certificates and other information relevant to certificates

Responsible officer in relation to a CA

A person occupying a position of responsibility in relation to the activities of the CA relevant to the regulation.

Sign and Signature

Include any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating or approving a record

Subscriber

Means a person (who may be a CA) who

(a) is named or identified in a certificate as the person to whom the certificate is issued;

(b) has accepted that certificate; and

(c) holds a private key which corresponds to a public key listed in that certificate

Trustworthy System

Means computer hardware, software and procedures that

(a) are reasonably secure from intrusion and misuse;

(b) are at a reasonable level in respect of availability, reliability and ensuring a correct mode of operations for a reasonable period of time;

(c) are reasonably suitable for performing their intended function; and

(d) adhere to generally accepted security principles.

Verify a Digital Signature

In relation to a given digital signature, electronic record and public key, means to determine that

(a) the digital signature was generated using the private key corresponding to the public key listed in a certificate; and

(b) the electronic record has not been altered since its digital signature was generated and any reference to a digital signature being verifiable is to be construed accordingly.

INTRODUCTION

In electronic transactions performed over an open network such as the Internet, there is a need for the parties involved to be assured of the identities of the transacting parties in the electronic environment. There is also a need to ensure that the electronic transactions are reliable and have not been tampered with.

Public key technology provides the capabilities for transacting parties in an electronic environment to authenticate each other's identities and ensure non-repudiation of electronic transactions through the use of digital signatures.

A certification authority acts as a trusted party to facilitate the confirmation of the relationship between a public key and a named entity. The certification authority issues digital certificates that can be used for authentication and digital signatures. The certification authority also performs certificate management services such as publication and revocation of digital certificates.

As certification authorities play a vital role in facilitating secure electronic transactions, there needs to be assurance that the certification authorities perform their roles and duties with high levels of integrity and security.

This document defines the security guidelines for the management, systems and operations of a certification authority. It is intended for use by the management, security, technical and operational personnel of a certification authority. It is assumed that the reader has basic understanding of public key technology and certification authority. The document makes reference to the BS 7799-1:2000 on general IT systems and operations.

The Controller of Certification Authorities ("the Controller") is the regulatory authority that supervises the activities of certification authorities in Nigeria.

Pending the establishment of the Nigeria Electronic Transaction Act (NETA) and its Regulations, NITDA as the Root CA and Controller of CAs for Nigeria would like to put in place a voluntary licensing scheme for Certificate Authorities (CAs) in Nigeria in addition to laying down the administrative framework for licensing as the Controller of CAs. The Regulations stipulates the criteria for a CA in Nigeria to be licensed, and the continuing operational requirements after obtaining a license.

This Regulation contains general information and is intended to guide interested organizations (public and private) in applying to be accredited CA.

Certification Authorities that intend to be licensed by the Controller shall comply with the mandatory requirements stated in this document.

This document will be reviewed on an ongoing basis to take into account the evolution of security and other related technologies.

Comments on this document can be forwarded to:

Controller of Certification Authorities

National Information Technology Development Agency (NITDA)

28, Port-Harcourt Crescent, Off Gimbiya Street, Area 11, Garki, Abuja, Nigeria

Email: cca@nitda.gov.ng

Website: http://www.nitda.gov.ng /

BENEFITS (ADVANTAGES) OF LICENSING

Although the licensing is a voluntary scheme, the regulation provides some benefits for Licensed CA.:

Evidentiary Presumption

Licensed CA will enjoy the benefits of evidentiary presumption for digital signatures generated from the certificate it issues. Without such presumption, a party that intends to rely on a digital signature must produce enough evidence to convince the court that the signature was created under condition that will guarantee it trustworthy. With the presumption, the party relying on the signature merely has to show that the signature has been correctly verified and the onus is on the other party disputing the signature to prove otherwise.

Liability of Licensed CAs

The liabilities of Licensed CAs are limited under this regulation. The CA will not be liable for any loss caused by reliance on a false or forged digital signature of a subscriber as long as the CA has complied with the requirements in this regulation.

Mark of Accreditation

The licensing of a CA by the Controller of CA is an indication that the CA has met the stringent regulatory requirements established. It is an indication to the public that the CA is trustworthy and deserving of consumer confidence. With the ease of proof in using digital signatures, the CA will enjoy public reliance with greater certainty.

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITY

MANAGEMENT GUIDELINES

CA plays an important role in a PKI as a trusted party which digital certificates derive legitimacy. It is essential to ensure that the management of a CA is proper and secure.

The scope of the management guidelines includes personnel, material, financial and information management guidelines.

Obligations

- Any CA function or service that is outsourced shall comply with the security guidelines. The outsourced function or service shall be audited for compliance with the guidelines.

- Accurate and complete records and transaction logs pertaining to the CA's business and operations shall be maintained. The records and logs shall be retained for the minimum period as specified in the applicable laws.

- Any "force majeure" provision in the CPS or other contractual agreement that relieves the CA of its obligations from events that are beyond reasonable control shall be brought to the attention of the user community.

- The user community shall be informed of the procedures for certificate registration, issuance, suspension and revocation.

- The subscribers shall be informed of their responsibility to verify the accuracy of the information contained in their certificates upon issuance.

- The subscriber's explicit consent shall be given before the CA can publish his certificate on the repository.

- Adequate information on the measures to protect the subscribers' private keys shall be provided to the subscribers. The implications of the different protection measures shall be brought to the attention of the subscribers.

- The subscribers' records shall be kept current and any changes in the information contained in the subscribers' certificates shall be updated promptly.

- The relying party shall be informed of the reasonable steps to be taken to verify the authenticity and validity of a certificate. The steps shall include verification of the following information in the certificate:
    1. Issuer's signature
    2. Policy parameters;
    3. Usage parameters;
    4. Validity period; and
    5. Revocation or suspension information.

- The user community shall be informed of the time intervals between each update and publication of the certificate suspension, certificate revocation and certificate revocation list information. The publication of such information shall conform to the time intervals specified.

Liability

- The user community shall be informed of the scope and limitations of CA's liabilities with respect to the expected reliance to be placed in the information contained in the certificates.

CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT (CPS)

- The user community shall be informed of the CA's Certificate Policy and Certification Practice Statement and any updates thereafter. The significance and implications of the Certificate Policy and Certification Practice Statement shall be brought to the attention of the user community.

- A Certificate Policy shall be defined for each class of certificates that have common assurance levels and usage requirements.

- Each Certificate Practice Statement shall be referenced by a unique object identifier (OID) approved by the Controller.

SECURITY MANAGEMENT

- The IT security policy for the CA organisation shall be defined and approved by the top management. The policy shall be communicated to all personnel and widely published throughout the organisation to ensure that the personnel are aware and reminded of the policy.

- Personnel shall be provided with the information security policy upon employment. It shall be the responsibility of each personnel to read and understand it. Security notices, pamphlets, posters and signs shall be used to provide updates and reminders of the security policy.

- An information security awareness program shall be implemented and conducted on at least an annual basis to ensure that all personnel are informed of the potential security risks and exposures in the CA operations and systems. In particular, personnel, especially those in the frontline service, shall be informed of typical social engineering attacks and the safeguards against them.

- All personnel shall be educated on basic IT principles and safeguards. Personnel responsible for security areas (e.g. systems and operations security administrator) shall be trained on advanced IT security principles and safeguards. The security personnel shall be trained in the security features and vulnerabilities of the systems and operations.

- Procedures shall be documented and implemented to ensure that when personnel or contractors are transferred by appointment, assignment or deployment, all access privileges to IT systems, information and assets are reviewed, modified or revoked accordingly.

- Procedures or a mechanism shall be established and implemented so that access rights of all registered users, their levels of access and their continued requirement for access can be checked on a regular basis (re-authentication).

- Procedures shall be established and implemented to actively keep track of security vulnerabilities and attacks that are reported by reputable sources and develop countermeasures or correct them promptly. The procedures should include an incident response capability to provide active defence and corrective actions against security exploits and attacks.

- Incident response procedures shall be established for documenting an event as a basis for subsequent action including forensics where necessary

Risk Management

- The components of the CA infrastructure (e.g. cryptographic algorithm and its key parameters, physical security, system security, operating system, etc.) shall be reviewed every year for new technology risks and appropriate action plans of the components shall be developed to manage the risks identified.

- Comprehensive CA system review, in the event of a hardware configuration change, software (operating system or layered product) update, network change (hardware, network operating system software or configuration), application update (new application or revised existing application) or changes made to the environment (physical or business) in which the CA functions, shall be conducted periodically.

- Risk management policies and procedures shall be reviewed periodically as part of a comprehensive risk management approach.

- Network and system security audits shall be performed periodically using automated audit tools to help identify new security vulnerabilities.

- Network penetration tests shall be performed periodically to help identify gaps that may have been introduced in the network perimeter defences .

- Intrusion detection systems shall be used to provide real time detection of network attacks.

- Risk analysis and protection policies shall be reviewed periodically for all incidents (real or suspected) or when the perceived threat level changes (technical, physical or personnel).
- Results and action plans, from the regular security audits and network penetration tests conducted by a suitably qualified independent party, shall be submitted to the Controller annually

Personnel Control

- All job applicants shall be subjected to security screening prior to being employed. The screening shall ensure that the applicant does not have any criminal records that may jeopardise the trustworthiness of the CA functions

- All personnel shall be required to sign a confidentiality agreement as part of their initial terms and conditions of employment prior to being given access to the CA services and processes facilities.

- Confidentiality or non-disclosure agreements shall be reviewed when there are changes to the terms of employment or contract, particularly when employees are due to leave the organization or contracts are due to end.

- All personnel shall be subjected to security re-screening at the point of relicensing in the case of a licensed CA, to ensure that they continue to be trustworthy.

- Personnel performing trusted roles or security-sensitive functions shall be subjected to stringent security screening (e.g. character profile).

- Dual control and segregation of duties shall be implemented for critical CA services and processes. In particular, technical personnel involved in critical CA services and processes such as the CA system administrators and operators shall not be given security related roles.

- Security related roles shall be given to dedicated personnel who are adequately trained to perform the job without any conflict of interest.

- Job responsibilities and access rights shall be designed and reviewed yearly to ensure proper segregation of duties and alignment of access rights to business functions, i.e. certificate registration, issuance, suspension and revocation. In addition, periodic cross checks on personnel performing trusted roles or security sensitive functions for incompatible duties or interests (internal or external) shall be conducted.

- All personnel shall be adequately trained in their designated tasks and functions. Personnel who have not been adequately trained shall not be allowed to independently operate the CA functions without the presence or supervision of trained personnel.

Maintenance of Subscribers' Data

- Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the CA's custody shall be implemented. Confidential information provided by the subscriber must not be disclosed to a third party without the subscribers' consent, unless the information is required to be disclosed under the law of the Federal Republic of Nigeria or a court order.

- Data on the usage of the certificates by the subscribers and other transactional data relating to the subscribers' activities generated by the CA in the course of its operation shall be protected to ensure the subscribers' privacy.

- Information resources shall be monitored to minimise risk of corruption and unauthorised disclosure, access, modification or deletion.

- Database management tools shall be used to manage and monitor information resources and master files.

Incident Management

- An incident management plan shall be developed and approved by the management. The plan shall include but not limited to the following areas:

    1. RA key compromise;
    2. CA certification key compromise;
    3. User certificate compromise;
    4. Systems and network penetration;
    5. Breach of physical security;
    6. Infrastructure availability; and
    7. Fraudulent registration and generation of certificates, certificate suspension and revocation information.

- An incident response action plan shall be established and periodically tested to ensure the readiness of the CA to respond to incidents. The plan shall include but not limited to the following areas

:

    1. Compromise control;
    2. Notification to user community; (if applicable)
    3. Revocation of affected certificates; (if applicable)
    4. Personnel incident handling responsibilities;
    5. Service disruption procedures and investigation;
    6. Monitoring and audit trail analysis; and
    7. Media and public relations.

- The CA's certificate shall be revoked immediately in the event of loss or compromise of the CA certification key or its storage device. All certificates signed using the CA's certification key shall be revoked.

- All incidents shall be reported to the Controller within 24 hours.

Business Continuity Planning

- Business continuity and disaster recovery planning shall be developed and tested periodically to ensure the continued availability of critical services in the event of a disaster or computer failure.

- The planning shall include continuity plans in the event of CA certification key loss and compromise.

- The personnel in the recovery team shall be provided with adequate training to deal with the crisis.

- The CA shall provide backup procedures and eliminate service failures as a result of "force majeure" not excluded from their obligations.

- Redundant systems and devices shall be available to ensure continued operation of critical services in a timely manner.

- The "hot" disaster recovery location shall have adequate security in place.

- Business continuity plans shall be reviewed for relevance and adequacy every six months to assure the continuity of business in the event of an emergency. Evidence of the review shall be documented for management review.

CERTIFICATE MANAGEMENT GUIDELINES

The certificate management processes include certificate registration, generation, issuance, renewal, suspension and revocation, as well as the publication of certificates, certificate suspension and revocation information. The objective is to establish integrity and accountability of the certificate management processes and the certificates.

Certificate Attributes

- A certificate shall be uniquely identifiable within its user community.
- A certificate shall indicate certificate policy and usage parameters to allow relying parties to check the acceptable use of a certificate.
- A certificate shall indicate expiration parameters to allow relying parties to verify validity of the certificate.
- The certificate should include parameters declaring the policy mapping as well as any constraints to policy maps.
- Sensitive personal information on the certificate user should not be provided in the certificate attributes such as in the distinguished names fields so as to protect the privacy of the user against potential social engineering infringements.
- Certificate extensions may be labelled as critical. The relying party shall be provided with the applications to verify and process any critical certificate extensions or reject the certificate.
- Certificate extensions should be used to:

    1. Identify the policies under which a certificate is issued;
    2. Map equivalent policies in different user communities or domains;
    3. Require subsequent certificates in a certification path to include specific policy identifiers or policy mappings;
    4. Limit the subject name space for subsequent certificates in the certification path;
    5. Restrict key usage;
    6. Limit number of subsequent certificates; and
    7. Distinguish between a CA certificate and a user certificate.

Registration

- The authentication method to verify the identity of the certificate applicant shall commensurate with the level of assurance accorded by the certificate. Where possible, face-to-face authentication of the applicant should be employed. A pre-existing trust relationship between the RA and the applicant may also be employed.

- The authenticity of attribute information of an applicant shall be verified against official documents issued by authorised organisations.

- Adequate documents and logs for each registration shall be maintained to enable post verification of the certificate applications.

Generation

- Procedures shall be defined to ensure that the subscribers' certificates generated are in accordance with the Certificate Policy.

- The accuracy (e.g. the information in the certificate is correct) and integrity (e.g. the correct association of the key pair with the certificate information) of the certificate shall be ensured.

Issuance

- A secure communication channel between the CA and its subscribers shall be established to ensure the authenticity, integrity and confidentiality of the exchanges (e.g. transmission of certificate, password, private key) during the certificate issuance process.

- The CA shall require the subscriber to explicitly acknowledge the receipt and acceptance of the certificate upon issuance.

Publication

- The CA shall publish its certificate and the location(s) of its CPS and repository to its user community using a reliable and trustworthy channel. (e.g. secure online mechanism or on a reputable newspaper).

- The CA shall publish at least the following information to allow its user community to verify the authenticity of the establishment operating the CA:

    1. Company name and registration number;
    2. X.500 name;
    3. Internet address;
    4. Telephone hotline number;
    5. CA certificate (or fingerprint of the certificate)
    6. Location(s) of the repository

- Publication of the subscribers' certificate information in the repository shall be subject to the subscribers' explicit consent.

- The contents in the repository shall be protected from unauthorised modification, insertion and deletion. Strong authentication mechanisms shall be used to validate identity of parties amending the repository contents. Where required, appropriate access controls to the contents of the repository shall be implemented to restrict access solely to the user community or to protect subscribers' privacy.

- Adequate backup and redundancy measures shall be implemented to ensure that the availability of the certificate repository conforms to the service level guaranteed to the user community.

Renewal

- The CA shall provide prior notice to the subscribers on the expiry date of their certificates so that they have sufficient time to apply for renewal or termination.

- Certificate renewal requests shall be submitted using a secure communication channel. A secure channel may include the use of an online renewal request that is digitally signed by the subscriber as long as the certificate is still valid.

- The certificate generation and issuance guidelines in this section shall apply in the generation and issuance of a new certificate to replace an expired certificate

.

Certificate Suspension

- A certificate shall be suspended in the event of suspected compromise of a subscriber's private key. A suspended certificate should only be reactivated when investigations established that no compromise has occurred.

- Certificate suspension requests shall be submitted using a secure communications channel to verify the identity of the requester so as to minimise risk of sabotage with unauthorised disruption of service or with malicious requests for suspension.

- Certificate suspension information in the certificate revocation list shall include the reason and time of the suspension so that relying parties can determine the point at which the certificate cease to be valid.

- Certificate suspension information in the certificate revocation list shall be digitally signed by the CA to enable the relying parties to verify the authenticity and integrity of the information.
- Certificate suspension information in the certificate revocation list shall be published once the suspension request has been verified to be valid.

- Certificate suspension information in the certificate revocation list shall be protected from unauthorised modification and deletion.

- The subscriber whose certificate has been suspended shall be notified once the suspension takes effect.

Certificate Revocation

- Permanent revocation occurs when a subscriber requests revocation for any reason. The CA shall state in its Certificate Policy whether an authorised representation of the policy making body or another member of the community that is subject to the Certificate Policy should be permitted to request the revocation of a certificate issued under the Certificate Policy. For example, the RA may be permitted to trigger the revocation of a certificate.

- Required revocation occurs when any party reasonably determines that a certificate is unreliable. A certificate shall be revoked under the following circumstances:

    1. Whenever any information marked with the extension “critical” on the certificate is no longer accurate;
    2. Whenever the private key associated with the certificate or the media holding the private key is, or is suspected of having been, compromised;
    3. Whenever the subscriber is no longer a member of the community that is subject to the Certificate Policy (e.g. cessation of employment or death);
    4. Upon the request of the subscriber;
    5. If the CA determines that the certificate was not properly issued in accordance with the CPS;
    6. If the certificate issuer or CA ceases operation; and • If the CA certification key is compromised.

- Certificate revocation requests shall be submitted using a secure communication channel to verify the identity of the requester so as to minimise risk of sabotage with unauthorised revocation.

- The certificate revocation information shall at least contain the following:
    1. Reason code for revocation; and
    2. Revocation date and time.

- Certificate revocation information shall be digitally signed by the CA to enable the relying party to verify the authenticity and integrity of the information.

- Certificate revocation information shall be published once the revocation request has been verified to be valid. It should include provisions for:
    1. Online certificate revocation checking; and
    2. Distribution points certificate revocation information.

- Certificate revocation information shall be protected from unauthorised modification and deletion.

- The subscriber who certificate has been revoked shall be notified once the revocation takes effect

- Revoked certificates shall not be re-activated.

Archival

- All certificate suspension and revocation information, certificates and their registration documents shall be archived for a minimum retention period of seven years in accordance with the applicable regulatory requirements so as to facilitate verification of digital signatures corresponding to certificates that have expired.

- Digital archives shall be indexed, stored, preserved and reproduced so as to be accurate, complete, legible and accessible to authorised persons. The integrity and availability of the digital archives shall be ensured.

Audit trails

- Audit trails of certificate registration, generation, issue, renewal, suspension and revocation shall be maintained.

- The integrity and availability of the audit trails shall be ensured.

- A reviewer tasked with the operational oversight role shall periodically review the certificate management audit trails to ensure normal operation and investigate suspicious activities.

- Audit trails shall be archived for a minimum period of twelve months or longer, in accordance with the applicable regulatory requirements.

KEY MANAGEMENT GUIDELINES

This section defines the guidelines to manage risk at each phase of key management to ensure confidentiality and integrity of cryptographic keys. It covers technical and administrative security requirements to manage risk of cryptographic key compromise. The scope includes cryptographic keys used by the certification authority (including registration functions) and the user community. The principle of split control is to be applied to the handling of CA keys.

Generation

- The subscriber's key pair shall be generated by the subscriber or on a key generation system. If the subscriber generates his own key pair, the CA shall approve the key generation system used.

- The CA keys shall be generated and stored under split control by parties who are not involved in the set-up and maintenance of the CA systems and operations.

- Separate key pairs for digital signature and encryption should be generated

.

- The key generation process shall generate statistically random key values for the generation of a strong (unique) key

.

Distribution

- Keys shall be transferred from the key generation system to the storage device (if the keys are not stored on the key generation system) using a secure mechanism that ensures end-to-end confidentiality and integrity.

Storage

- The CA should provide the subscriber with the equipment and programs to securely store the subscriber's private key in an encrypted form.

- CA keys shall be stored in tamper-proof devices and can only be activated under split control by parties who are not involved in the set-up and maintenance of the CA systems and operations. The CA key may be stored in a tamper-proof cryptographic module or split into sub-keys stored in tamper-proof devices under the custody of the key custodians.

- The CA key custodians shall ensure that the CA key component or the activation code is always under his sole custody. Change of key custodians shall be approved by the CA management and documented. In the event that the key custodian is unavailable,

- CA should put in place a system of checks to ensure that there is no single point of failure.

Usage

- A system and software integrity check shall be performed prior to CA key loading.

- Custody of and access to the CA keys shall be under split control. In particular, CA key loading shall be performed under split control.

Backup

- CA private keys shall be backed up to prevent a CA's operation from stopping due to accidental deletion or corruption of keys.

- CA private key backups shall be protected with the same guidelines as required for CA private key storage.

- Separate key custodians shall be assigned to protect each component of the backup key.

- CA private key backups should be stored in a separate secure storage facility, at a different location from where the original key is stored.

Key Change

- CA and subscriber keys shall be changed or recertified periodically.

- Key change shall be processed as per Key Generation guidelines.

- The validity period shall be defined.

- The CA shall provide reasonable notice to the subscriber's relying parties of any change to a new key pair used by the CA to sign certificates.

- The CA shall define a CA key change process that ensures reliability of the process by showing how the generation of key interlocks – such as signing a hash of the new key with the old key.

- The CA shall notify the subscriber or the owner of the digital certificates of any type of key change that are performed automatically either through a secure application program or outsourced mode.

Destruction

- Upon termination of use of a CA signature private key, all components of the private key and all its backup copies shall be securely archived and stored in a secure location.

Key Compromise

- A procedure shall be pre-established to handle cases where a compromise of the CA certification key has occurred. (See Incident Management)

- The CA shall immediately revoke all affected subscriber certificates in the case of CA certification private key compromise.

- The CA shall immediately revoke the affected keys and certificates in the case of subscriber private key compromise.

CA Key and Subscriber Encryption Key Archival

- CA Public keys shall be archived permanently to facilitate audit or investigation requirements.

- All subscriber encryption keys should be archived for a reasonable period of time to safeguard users from any compromise or misplacement of keys that may result in their own denial of service.

- Archives of CA public keys and subscriber encryption keys shall be protected from unauthorised modification.

Cryptographic Engineering

- The cryptographic processes for the CA operations shall be performed in a hardware cryptographic module that minimally conforms to FIPS 140-1 Security Level 3 or FIPS 140-2 Security Level 3.

- If the RA's operations are separate from the CA, its cryptographic processes shall minimally conform to FIPS 140-1 Security Level 2 or FIPS 140-2 Security Level 2.

- The cryptographic processes for the subscriber's operations shall minimally conform to FIPS 140-1 Security Level 1 or FIPS 140-2 Security Level 1.

- All cryptographic algorithms, protocols and their implementations shall be reviewed by a suitably qualified independent party to ensure that the cryptographic components are sufficiently secure and correctly implemented. The components that require certification include all modules and components involved in key generation, key storage, key transport and key usage.

- The cryptographic keys and algorithms shall be sufficiently strong to protect the cryptographic result (e.g. digital signature) from attacks for the life span of the keys.

- The asymmetric cryptographic algorithms used should conform to the IEEE Standard Specifications for public key cryptography [IEEE1363].

SYSTEMS AND OPERATIONS GUIDELINES

Design, configuration, operation and maintenance of systems and networks are critical to the security of IT-enabled businesses, especially a CA whose core business revolves around the use of computer systems and networks to provide trusted services for digital certificates. The guidelines listed here are intended to be specific to the CA services and to supplement the general IT security controls addressed in the BS 7799-1:2000. The scope includes availability, confidentiality, integrity and access control of critical CA systems and operations.

Physical Security

- Responsibilities for the physical security of the CA systems shall be defined and assigned to named individuals.
- The location of the CA system shall not be publicly identified.
- Physical access security systems shall be installed to control and audit access to the certification system.
- Dual control over the inventory and access cards/keys shall be in place. An upto-date list of personnel who possess the cards/keys shall be maintained.
- Cryptographic keys under the custody of the key custodians shall be physically secured from unauthorised access, use and duplication.
- Loss of access cards/keys shall be reported immediately to the security administrator; who shall take appropriate actions to prevent unauthorised access.
- CA systems should be located in an area away from strong sources of magnetic or radio frequency interference.
- Systems performing the certification function shall be located in a dedicated room or partition to facilitate the enforcement of physical access control.
- Entry and exit of the room or partition shall be automatically logged with timestamps and be reviewed by the CA security administrator daily.
- Access to infrastructure components essential to functioning of CA systems such as power control panels, communications risers and cabling shall be restricted to authorised personnel.
- Adequate approval procedures and compensating controls shall be in place at times (e.g. during emergency situations) when it is necessary to temporarily bypass or de-activate normal physical security arrangements.

- Bypass or de-activation of normal physical security arrangements shall be authorised and recorded by security personnel.

- Suitable intrusion detection systems installed to professional standards and periodically tested shall be used to monitor and record physical access to the certification system during after hours. Unoccupied areas should be alarmed at all times and cover should be provided for all other areas.

Systems and Software Integrity and Control

- Systems performing the certification function shall be dedicated to that function and not be used for other purposes (e.g. web surfing, word processing).

- Systems and application software shall be verified for integrity before each execution.

- Systems and application software shall minimally conform to Common Criteria EAL4 or equivalent security level.

- Systems shall enforce strong authentication mechanisms that are not susceptible to prediction, dictionary attacks or replay.

- The security-critical software, that includes, but not limited to, software that has a crypto module embedded, shall be reviewed by a suitably qualified independent party.

- Personnel shall be appropriately trained on the secure and proper operation of CA applications.

- Automatic time-out for terminal inactivity should be implemented. For sensitive systems, the time-out should be not longer than 10 minutes.

Change and Configuration management

- Executables of questionable sources or where trustworthiness cannot be ascertained shall not be installed or run on CA systems.

- Software updates and patches shall be reviewed, thoroughly tested and proven for security implications before being implemented

- Software updates and patches to rectify security vulnerabilities in critical systems shall be promptly reviewed and implemented.

- The information on the software updates and patches and their implementation shall be clearly and properly documented.

Network and Communications Security

- CA systems shall be protected to ensure network access control to critical systems and services from other systems.

- Network connections to external networks (if required) from the CA systems shall be restricted to only the connections that are essential to facilitate CA functional processes and services.

- Network connections (if required) should be initiated by the systems performing the certification function to those performing the registration and repository functions but not vice versa. If this is not possible, compensating controls (e.g. use of proxies) shall be implemented to protect the systems performing the certification function from potential attacks

- Security testing and evaluation of the network access control of the CA systems shall be reviewed by a suitably qualified independent party before allowing connections to the external network to be made. Mitigating controls shall be put in place for the risks that have been identified.

- Systems performing the certification function should be isolated to minimize exposure to attempts to compromise the confidentiality, integrity and availability of the of the certification function.

- The CA certification key shall be protected from unauthorised access to ensure its confidentiality and integrity.

- Communications between the CA systems over a network shall be secure to ensure confidentiality, integrity and authenticity. For example, communications between the CA systems over a network should be encrypted and digitally signed.

- Intrusion detection tools shall be deployed to monitor critical networks and perimeter networks and alert administrators of network intrusions and penetration attempts in a timely manner.

Monitoring and Audit Logs

- The CA should consider the use of automated security management and monitoring tools providing an integrated view of the security situation at any point in time.

- Records of the following application transactions shall be maintained:
    1. Registration;
    2. Certification;
    3. Publication;
    4. Suspension; and
    5. Revocation.

- Records and log files shall be reviewed periodically for the following activities:
    1. Misuse;
    2. Errors;
    3. Security violations;
    4. Execution of privileged functions;
    5. Change in access control lists;
    6. Change in system configuration; and
    7. Change in software modules.

- Review of audit trails shall be performed by personnel tasked specifically with the oversight function.

- Audit logs shall be adequately protected from unauthorised access, modification and deletion and backed up periodically in a timely manner for archival purposes.

- Audit trail retention for system access records (e.g. Syslog, security–related logs) shall be kept for a minimum of twelve months or longer, in either hard copy or electronic form. Records that are necessary to support litigation or investigation of criminal activities shall be retained permanently or as stipulated by relevant legislations.

- Records of applications transactions and significant events shall be retained for a minimum of twelve months or longer, in accordance with the applicable regulatory requirements.

APPLICATION INTEGRATION GUIDELINES

This section defines guidelines to the certification authority for application toolkits to ensure secure implementation and operation. The scope includes toolkits provided by the CA to the user and developer community. Verification of certificates is addressed in this section and not Certificate Management because it is not a CA function but a function of the applications used by the user community.

Integrity of Signing and Verification Functions

- The application shall inform the user when a private key is being accessed.
- The user shall be alerted if its private key is being used for a purpose that is not consistent with that defined as acceptable use by the issuer.
- Mechanism shall be available to check the integrity of the applications for unauthorised modifications, especially. the integrity of signing and verification functions.
- Application security risk assessment on the CA's software infrastructure should be conducted yearly to ensure that the CA software that manages, issues and revokes certificates is developed to manage the risk identified.
- The application should be reviewed by a suitably qualified independent party to ensure safe operations.

Protection of Private Key

- The RA private keys shall be stored in tamper-evident devices and protected from unauthorised use or copy.
- The CA private keys shall be stored in tamper-proof devices and protected from unauthorised use or copy.
- Application should securely purge the private key temporarily stored for processing to minimise private key exposure

.

Verification of Certificates

- The application shall verify the validity and authenticity of the certificate.
- The verification process shall trace and verify all the components in the certification path.

- The relying party should be informed of what a particular assurance level means, how the private key associated with the certificate is stored, how entities are verified and the issuance process.

  (a) For validity and authenticity verification, it shall be necessary to verify that:
  1. The certificate issuer's signature is valid;
  2. The certificate is valid (i.e. has not expired, been suspended or revoked); and
  3. The certificate extensions flagged as "critical" are being complied with.

APPLICATION FORM FOR

ACCREDITATION OR RENEWAL OF ACCREDITATION OF CERTIFICATION AUTHORITY

This application form is for Certification Authorities who desire to be accredited, or who desire to renew their accreditation, under the Certification Authority Regulations.

SECTION 1 – COMPANY DATA

Company Name: _____

_____

Address in Nigeria _____

_____

:

Tel No: +234_____

RC No: _____ Date of Registration: (DD/MM/YYYY)

Registered as:

___ Public Limited (limited by shares)
___ Private Limited (non-exempt limited by shares)
___ Others (please specify):

Principal business activities:

_____
_____
_____
_____

URL of web site: http(s)://www._____

Please attach the following:

(a) A recent Company Profile with evidence of possessing both human and technical resources required as CA (ICT Infrastructure and Personnel)
(b) Company organizational structure, including names and resume of key personnel
(c) *CAC Certificate.*
(d) *Genuine Tax Clearance Certificate for the last 3 years.*
(e) *Certified True Copies of Article and Memorandum of Association, Form CO2 and CO7*
(f) *Verifiable Evidence of financial capability supported with bank statements for the last 6 months from a commercial bank.*
(g) *A certified true copy of the applicant company's resolution(s):*
- *to apply as an accredited Certification Authority ("**CA**"), or (in the case of an accredited CA applying for renewal of its accreditation) for renewal of its accreditation; and*
- *to authorize, for the purpose of making this application on the applicant company's behalf, the person(s) making the application.*

SECTION 2 – COMPANY OWNERSHIP

Board of Directors

Name	Position	Percentage of Shares	Home Address	Phone Number(s)
	Chairman			
	CEO			
	Company Secretary			
	Director			
	Director			

SECTION 3 – POLICIES AND OPERATIONS

Please provide a copy of the following:

1. Certification Practice Statement of the CA (CPS)
2. Technical specifications of the CA system
3. CA's public key certificate (hardcopy and softcopy)
4. CA's security policies and standards
5. CA's incident management plan
6. CA's business continuity plan
7. Audit report prepared in accordance with the Regulations for compliance
8. Auditors Credentials

SECTION 4 – PERSONNEL

Please provide a copy of the following:

1. Name(s)
2. International Passport Number
3. Verifiable Residential Address
4. Designation and function
5. Date of Employment
6. Details of qualifications and experience to carry out his/her duties as a trusted person.

SECTION 5 – INSOLVENCY AND LEGAL PROCEEDINGS

Has the applicant company ever been involved in any legal proceedings or dispute settlement in Nigeria or anywhere else in the world in its capacity as a Certification Authority?

____ YES _____ NO

If yes, please furnish complete details. (Please attach a separate sheet of paper if the space provided is inadequate)

_____
_____
_____
_____
_____

Is the applicant company in the of being wound up or liquidated?

____ YES _____ NO

If yes, please furnish complete details. (Please attach a separate sheet of paper if the space provided is inadequate)

_____
_____
_____
_____
_____

Has the applicant company or any of the repective directors and key executives or any of the trusted persons, ever been convicted of an offence for which the conviction involved he/she acted fraudulently?

____ YES _____ NO

If yes, please furnish complete details. (Please attach a separate sheet of paper if the space provided is inadequate)

_____
_____
_____
_____
_____

SECTION 6 – CONTACT PERSON

Name: _____

Designation: _____

Tel No. _____

Email: _____

The contact person must be able to provide clarification or/and further information regarding the application to the Controller.

SECTION 7 – DECLARATION

In applying to the Controller of Certification Authorities in Nigeria to operate as an accredited Certification Authority under the Regulations, I declare that all the above information provided by the company is true and complete.

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

The Controller reserves the right to reject any application without providing any reason.

Name: _____

Designation: _____

Tel No. _____

Email: _____

Date: _____

Signature: _____
Company Stamp or Seal

Regulations

ACCREDITATION OF CERTIFICATION AUTHORITIES

Regulation 1- Application to be Accredited Certification Authority

1. Every application to be an accredited certification authority shall be made in such form and manner as the Controller may, from time to time, determine and shall be supported by:
    - the certification practice statement of the certification authority;
    - an audit report prepared in accordance with regulations 23 for compliance with the Compliance Audit Checklist published on back of this document (appendix 1) or the Controller's Internet website; and
    - such information as the Controller may require.

2. Upon submitting an application for accreditation, the applicant shall pay to the Controller an application fee of N1,000,000.

3. The Controller shall, in such form as the Controller may determine, notify the applicant as to whether his application is successful.

4. Upon notification that his application is successful, the applicant shall pay to the Controller an accreditation fee of N1,000,000 and, subject to regulation 3, the Controller shall grant accreditation to the applicant as an accredited certification authority upon such payment.

5. The accreditation shall be subject to such conditions or restrictions as the Controller may, from time to time, determine.

6. The accreditation shall be valid for a period of 2 years unless cancelled or suspended under these Regulations.

7. The Controller shall not refund any fee paid under this regulation if the application is unsuccessful, withdrawn or discontinued, or if the accreditation is cancelled or suspended.

Regulation 2 - Renewal of Accreditation

1. Regulation 1 shall apply, with the necessary modifications, to an application for renewal of accreditation under this regulation as it applies to an application for accreditation under regulation 1

.

2. The Controller may allow applications for renewal of accreditation to be submitted in the form of electronic records subject to such requirements as the Controller may impose.

3. If an accredited certification authority intends to renew its accreditation, the certification authority shall submit an application for the renewal of its accreditation not later than 3 months before the expiry of its accreditation.

4. If an application for renewal is made later than the time prescribed in paragraph (3), the application shall be deemed to be an application under regulation 1 and the application fee prescribed in regulation 1(2) shall be payable.

5. If the certification authority does not intend to renew its accreditation, the certification authority shall:
    - inform the Controller in writing not later than 3 months before the expiry of the accreditation;
    - inform all its subscribers in writing not later than 2 months before the expiry of the accreditation; and
    - advertise such intention in such daily newspapers and in such manner as the Controller may determine, not later than 2 months before the expiry of the accreditation.

REFUSAL, CANCELLATION AND SUSPENSION OF ACCREDITATION

Regulation 3 - Refusal to Grant or Renew Accreditation

The Controller may refuse to grant or renew an accreditation if:

1. The applicant has not complied with any requirement in these Regulations;

2. The applicant has not provided the Controller with such information relating to it or any person employed by or associated with it for the purposes of its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require;

3. The applicant or its substantial shareholder is in the course of being wound up or liquidated;

4. A receiver or a receiver and manager has been appointed to the applicant or its substantial shareholder;

5. The applicant or its substantial shareholder has, whether in Nigeria or elsewhere, entered into a compromise or scheme of arrangement with its creditors, being a compromise or scheme of arrangement that is still in operation;

6. The applicant or its substantial shareholder or any trusted person has been convicted, whether in Nigeria or elsewhere, of an offence the conviction for which involved a finding that it or he acted fraudulently or dishonestly, or has been convicted of an offence under these Regulations;

7. The Controller is not satisfied as to the qualifications or experience of the trusted person who is to perform duties in connection with the accreditation of the applicant;

8. The applicant fails to satisfy the Controller that it is a fit and proper person to be accredited or that all its trusted persons and substantial shareholders are fit and proper persons;

9. The Controller has reason to believe that the applicant may not be able to act in the best interest of its subscribers, customers or participants having regard to the reputation, character, financial integrity and reliability of the applicant or any of its substantial shareholders or trusted persons;

10. The Controller is not satisfied as to the financial standing of the applicant or its substantial shareholder;

11. The Controller is not satisfied as to the record of past performance or expertise of the applicant or its trusted person having regard to the nature of the business which the applicant may carry on in connection with the accreditation;

12. There are other circumstances which are likely to lead to the improper conduct of business by, or reflect discredit on the method of conducting the business of, the applicant or its substantial shareholder or any of the trusted persons; or

13. The Controller is of the opinion that it is in the interest of the public to do so.

Regulation 4 - Cancellation or Suspension of Accreditation

1. An accreditation shall be deemed to be cancelled if the certification authority is wound up.

2. The Controller may cancel or suspend the accreditation of a certification authority:

    - on any ground on which the Controller may refuse to grant an accreditation under regulation 3;
    - if any information furnished in support of the application for the accreditation was false, misleading or inaccurate;
    - if the certification authority fails to undergo or pass an audit required under these regulation;
    - if the certification authority fails to comply with a direction of the Controller made under these regulations;
    - if the certification authority is being or will be wound up;
    - if the certification authority has entered into any composition or arrangement with its creditors;
    - if the certification authority fails to carry on business for which it was accredited;
    - if the Controller has reason to believe that the certification authority or its trusted person has not performed its or his duties efficiently, honestly or fairly; or
    - if the certification authority contravenes or fails to comply with any condition or restriction applicable in respect of the accreditation.

3. The Controller may cancel the accreditation of a certification authority at the request of that certification authority.

4. The Controller shall not cancel the accreditation under paragraph (2) without first giving the certification authority an opportunity of being heard.

Regulation 5 - Inquiry into Allegations of Misconduct, etc.

1. The Controller may inquire into any allegation that a certification authority, its officers or employees, is or has been guilty of any misconduct or is no longer fit to continue to remain accredited by reason of any other circumstances which have led, or are likely to lead, to the improper conduct of business by it or to reflect discredit on the method of conducting business.

2. If, after inquiring into an allegation under paragraph (1), the Controller is of the opinion that the allegation is proved, the Controller may if he thinks fit:
    - cancel the accreditation of the certification authority;
    - suspend the accreditation of the certification authority for such period, or until the happening of such event, as the Controller may determine; or
    - reprimand the certification authority.

3. The Controller shall, at the hearing of an inquiry into an allegation under paragraph (1) against a certification authority, give the certification authority an opportunity of being heard.

4. Where the Controller is satisfied, after making an inquiry into an allegation under paragraph (1), that the allegation has been made in bad faith or that it is otherwise frivolous or vexatious, the Controller may, by order in writing, require the person who made the allegation to pay any costs and expenses involved in the inquiry.

5. The Controller may issue directions to the certification authority for compliance as a result of making the inquiry.

6. For the purposes of this regulation, “misconduct” means:

    - any failure to comply with the requirements of these Regulations or the certification practice statement of the certification authority concerned; and
    - any act or omission relating to the conduct of business of the certification authority concerned which is or is likely to be prejudicial to public interest.

Regulation 6 - Effect of Cancellation or Suspension of Accreditation

1. A certification authority whose accreditation is cancelled or suspended under regulation 5 or 6 shall, for the purposes these Regulations, be deemed not to be accredited from the date that the Controller cancels or suspends the accreditation, as the case may be.

2. The cancellation or suspension of the accreditation of a certification authority shall not operate so as to:
    - avoid or affect any agreement, transaction or arrangement entered into by the certification authority, whether the agreement, transaction or arrangement was entered into before or after the cancellation or suspension of the accreditation; or
    - affect any right, obligation or liability arising under any such agreement, transaction or arrangement.

Regulation 7 - Appeal to Minister

1. Where the Controller:
    - refuses to grant or renew an accreditation under regulation 3;
    - cancels or suspends an accreditation under regulation 4; or
    - cancels or suspends an accreditation, or reprimands a certification authority, under regulation 5,

    any person who is aggrieved by the decision of the Controller may, within 14 days after he is notified of the decision, appeal to the Minister and the decision of the Minister shall be final.

2. If an appeal is made against a decision made by the Controller, the Controller may, if he thinks fit, defer the execution of the decision until the appeal has been decided by the Minister or the appeal is withdrawn.

3. In considering whether to defer the execution of the decision, the Controller shall have regard to whether the deferment is prejudicial to the interests of any subscriber of the certification authority or any other party who may be adversely affected.

4. If an appeal is made to the Minister, a copy of the appeal shall be lodged with the Controller.

ACCREDITATION REQUIREMENTS

Regulation 8 - Business structure

An applicant for accreditation must be a company operating in Nigeria at the time of the application and throughout the period when it is an accredited certification authority.

Regulation 9 - Personnel

1. An applicant for accreditation shall, at the time of the application and throughout the period when it is an accredited certification authority, take reasonable measures to ensure that every trusted person:
    a. is a fit and proper person to carry out the duties assigned to him;
    b. is not an un-discharged bankrupt in Nigeria or elsewhere, and has not made any composition or arrangement with his creditors; and
    c. has not been convicted, whether in Nigeria or elsewhere, of :
        i. an offence the conviction for which involved a finding that he acted fraudulently or dishonestly; or
        ii. an offence under these Regulations.

2. Notwithstanding paragraph (1)(*c*), the Controller may allow the applicant or accredited certification authority to have a trusted person who has been convicted of an offence referred to in that paragraph, if the Controller is satisfied that:
    (a) the trusted person is now a fit and proper person to carry out his duties; and
    (b) 10 years have elapsed from:
    - the date of conviction; or
    - the date of release from imprisonment if he was sentenced to a term of imprisonment, whichever is the later.

3. Every trusted person must:
    (a) have a good knowledge of these Regulations;
    (b) be trained in the certification authority's certification practice statement; and
    (c) possess the relevant technical qualifications, expertise and experience to effectively carry out his duties.

Regulation 10 - Certification practice statement

An accredited certification authority must have and comply with a Certification Practice Statement (CPS) approved by the Controller.

CONDUCT OF BUSINESS BY ACCREDITED CERTIFICATION AUTHORITIES

Regulation 11 - Trustworthy Record Keeping and Archival

1. An accredited certification authority may keep its records in the form of paper documents, electronic records or any other form approved by the Controller.

2. Such records shall be indexed, stored, preserved and reproduced so as to be accurate, complete, legible and accessible to the Controller, an auditor or an authorised officer.

Regulation 12 - Trustworthy Transaction Logs

1. Every accredited certification authority shall make and keep in a trustworthy manner the records relating to:
    - activities in issuance, renewal, suspension and revocation of certificates (including the process of identification of any person requesting a certificate from an accredited certification authority);
    - the process of generating subscribers' (where applicable) or the accredited certification authority's own key pairs;
    - the administration of an accredited certification authority's computing facilities; and
    - such critical related activity of an accredited certification authority as may be determined by the Controller.

2. Every accredited certification authority shall archive all certificates issued by it and maintain mechanisms to access such certificates for a period of not less than 7 years.

3. Every accredited certification authority shall retain all records required to be kept under paragraph (1) and all logs of the creation of the archive of certificates referred to in paragraph (2) for a period of not less than 7 years.

Regulation 13 - Types of Certificates

1. Subject to the approval of the Controller, an accredited certification authority may issue certificates of the following different levels of assurance:
    - certificates which shall be considered as trustworthy certificates. and
    - certificates which shall not be considered as trustworthy certificates.

2. The accredited certification authority must associate a distinct certification practice statement approved by the Controller for each type of certificate issued.

3. The accredited certification authority must draw the attention of subscribers and relying parties to the effect of using and relying on certificates that are not considered trustworthy certificates.

Regulation 14 - Issuance of Certificates

1. Every accredited certification authority shall comply with the requirements in this regulation in relation to the issuance of certificates.

2. The certificate must contain or incorporate by reference such information as is sufficient to locate or identify one or more repositories in which notification of the suspension or revocation of the certificate will be listed if the certificate is suspended or revoked.

3. The practices and procedures set forth in the certification practice statement of an accredited certification authority may contain conditions with standards higher than those conditions specified in the Regulation

4. The subscriber identity verification method employed for issuance of certificates must be specified in the certification practice statement and is subject to the approval of the Controller during the application for accreditation.

5. Where a certificate is issued to a person (referred to in this regulation as the new certificate) on the basis of another valid certificate held by the same person (referred to in this regulation as the originating certificate) and subsequently the originating certificate has been suspended or revoked, the certification authority that issued the new certificate must conduct investigations to determine whether it is necessary to suspend or revoke the new certificate.

6. The accredited certification authority must provide a reasonable opportunity for the subscriber to verify the contents of the certificate before it is accepted.

7. If the subscriber accepts the issued certificate, the accredited certification authority shall publish a signed copy of the certificate in a repository referred to in paragraph (2).

8. Notwithstanding paragraph (7), the accredited certification authority may contractually agree with the subscriber not to publish the certificate.

9. If the subscriber does not accept the certificate, the accredited certification authority shall not publish it.

10. Once the certificate has been issued by the accredited certification authority and accepted by the subscriber, the accredited certification authority shall notify the subscriber within a reasonable time of any fact known to the accredited

certification authority that significantly affects the validity or reliability of the certificate.

11. The date and time of all transactions in relation to the issuance of a certificate must be logged and kept in a trustworthy manner.

Regulation 15 - Renewal of Certificates

1. Regulation 14 shall apply to the renewal of certificates as it applies to the issuance of certificates.

2. The subscriber identity verification method shall be that specified in the certification practice statement as approved by the Controller.

3. The date and time of all transactions in relation to the renewal of a certificate must be logged and kept in a trustworthy manner.

Regulation 16 - Suspension of Certificates

1. This regulation shall apply only to every accredited certification authority which allows subscribers to request for suspension of certificates.

2. Every accredited certification authority may provide for immediate revocation instead of suspension if the subscriber has agreed in writing.

3. Upon receiving a request for suspension of a certificate in accordance with the Regulation, the accredited certification authority shall ensure that the certificate is suspended and notice of the suspension published in the repository in accordance with the Regulation

4. An accredited certification authority may suspend a certificate that it has issued if the accredited certification authority has reasonable grounds to believe that the certificate is unreliable, regardless of whether the subscriber consents to the suspension; but the accredited certification authority shall complete its investigation into the reliability of the certificate and decide within a reasonable time whether to reinstate the certificate or to revoke the certificate in accordance with the Regulation.

5. It is the responsibility of any person relying on a certificate to check whether a certificate has been suspended.

6. An accredited certification authority shall suspend a certificate after receiving a valid request for suspension (in accordance with the Regulation); but if the accredited certification authority considers that revocation is justified in the light

of all the evidence available to it, the certificate must be revoked in accordance with the Regulation.

7. An accredited certification authority shall check with the subscriber or his authorised agent whether the certificate should be revoked and whether to reinstate the certificate after suspension.

8. An accredited certification authority must terminate a suspension initiated by request if the accredited certification authority discovers and confirms that the request for suspension was made without authorisation by the subscriber or his authorised agent.

9. If the suspension of a certificate leads to a revocation of the certificate, the requirements for revocation shall apply.

10. The date and time of all transactions in relation to the suspension of certificates must be logged and kept in a trustworthy manner.

11. An accredited certification authority must maintain facilities to receive and act upon requests for suspension at all times of the day and on all days of every year.

Regulation 17 - Revocation of Certificates

1. In order to confirm the identity of the subscriber or authorised agent making a request for revocation, the accredited certification authority must use the subscriber identity verification method specified in the certification practice statement for this purpose.

2. An accredited certification authority must, after receiving a request for revocation, verify the request, revoke the certificate and publish notification of it.

3. An accredited certification authority must maintain facilities to receive and act upon requests for revocation at all times of the day and on all days of every year.

4. An accredited certification authority shall give notice to the subscriber immediately upon the revocation of a certificate.
5. The date and time of all transactions in relation to the revocation of certificates must be logged and kept in a trustworthy manner.

Regulation 18- Expiry Date of Certificates

A certificate must state the date on which it expires.

Regulation 19 - Maintenance of Certification Practice Statement (CPS)

1. Every accredited certification authority shall use the Internet draft of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, adopted by the Internet Engineering Task Force and reproduced by the Controller on its Internet website, as a guide for the preparation of its certification practice statement.

2. Any change to the certification practice statement during the term of the accreditation requires the prior approval of the Controller.

3. Every accredited certification authority must highlight to its subscribers any limitation of their liabilities and, in particular, it must draw the subscribers' attention to the implication of reliance limits on their certificates.

4. The subscriber identity verification method for the issuance, renewal, suspension and revocation of a certificate must be specified in the certification practice statement.

5. A copy of the latest version of the certification practice statement, together with its effective date, must be filed with the Controller and published on the certification authority's Internet website accessible to members of the public.

6. After the effective date, the latest version filed with the Controller will be the prevailing version for a particular certificate.

7. Every accredited certification authority must log all changes to the certification practice statement together with the effective date of each change.

8. An accredited certification authority shall keep in a trustworthy 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.

Regulation 20 - Secure Digital Signatures

1. The technical implementation shall be such as to ensure that it is computationally infeasible for any person, other than the person to whom the signature correlates, to have created a digital signature which is verified by reference to the public key listed in that person's certificate.

2. The signature on its own should be such as to:
    - ensure that the name or other unique identifiable notation of the person to whom the signature correlates be incorporated as part of the signature and cannot be replaced or forged; and
    - readily present such indicia of identity to a person intending to rely on the signature.

3. The technical implementation should ensure that :
    - the steps taken towards the creation of the signature must be under the direction of the person to whom the signature correlates; and
    - no other person can reproduce the sequence of steps to create the signature and thereby create a valid signature without the involvement or the knowledge of the person to whom the signature correlates.

4. The technical implementation should indicate to a relying party of a signature whether the document or record that the signature purports to sign has been modified in any way and this indication should be revealed in the process of verifying the signature.

Regulation 21 - Compliance Audit Checklist

1. Every accredited certification authority shall ensure that in the performance of its services it materially satisfies the Compliance Audit Checklist determined by the Controller and published on the Controller's Internet website.

2. An auditor, when determining whether a departure from the Compliance Audit Checklist is material, shall exercise reasonable professional judgment as to whether a condition that does not strictly comply with the Compliance Audit Checklist is or is not material, taking into consideration the circumstances and the system as a whole.

3. Without prejudice to the generality of situations which the auditor may consider to be material, the following incidents of non-compliance shall be considered to be material:
    - any non-compliance relating to the validity of a certificate;
    - the performance of the functions of a trusted person by a person who is not suitably qualified; or
    - the use by an accredited certification authority of any system other than a trustworthy system.

4. The Compliance Audit Checklist shall be interpreted in a manner that is reasonable in relation to the context in which a system is used and is consistent with law.

5. Notwithstanding an auditor's assessment of whether a departure from the Compliance Audit Checklist is material, the Controller may make his own assessment and reach a conclusion for the purpose of paragraph (1) which is at variance with that of the auditor.

6. Every accredited certification authority shall provide every subscriber with a trustworthy system to generate his key pair.

7. Every accredited certification authority shall provide the mechanism to generate and verify digital signatures in a trustworthy manner and the mechanism provided shall also indicate the validity of the signature.

8. If the digital signature is not valid, the mechanism provided should indicate if the invalidity is due to the integrity of the document or the signature and the mechanism provided shall also indicate the status of the certificate.

9. For mechanisms provided by third parties other than the accredited certification authority, the resulting signature is considered secure only if the accredited certification authority endorses the implementation of such mechanisms in conjunction with its certificate.

10. Every accredited certification authority shall be responsible for the storage of keys (including the subscriber's key and the accredited certification authority's own key) in a trustworthy manner.

11. The Controller may, from time to time, publish on its Internet website further details of the Compliance Audit Checklist for compliance by every accredited certification authority.

Regulation 22 - Incident Handling

1. An accredited certification authority shall implement an incident management plan that must provide at the least for management of the following incidents:
    - compromise of key;
    - penetration of certification authority system and network;
    - unavailability of infrastructure; and
    - fraudulent registration and generation of certificates, certificate suspension and revocation information.

2. If any incident referred to in paragraph (1) occurs, it shall be reported to the Controller within 24 hours.

Regulation 23 - Confidentiality

1. Every accredited certification authority and its authorised agent must keep all subscriber-specific information confidential.

2. Paragraph (1) shall not apply to:
    - any disclosure of subscriber-specific information made:
    - with the permission of the subscriber;
    - for the purposes of the administration or enforcement of any part of the Regulation;
    - for any prosecution under any written law; or
    - in compliance with an order of court or the requirement of any written law; or any subscriber-specific information which:
        - is contained in the certificate, or is otherwise provided by the subscriber to the accredited certification authority, for public disclosure; or
        - relates to the fact that the certificate has been suspended or revoked.

Regulation 24- Change In Management

1. An accredited certification authority shall notify the Controller within 5 days of any changes in:
    - the appointment of any person as a member of its board of directors, its chairman or its chief executive, or their equivalent; or
    - any persons with a controlling interest in the certification authority.

2. For the purposes of paragraph (1)(*b*), a person has a controlling interest in a certification authority if:
    - that person has an interest in the voting shares of the certification authority and exercises control over the certification authority; or
    - that person has an interest in the voting shares of the certification authority of an aggregate of not less than 30% of the total votes attached to all voting shares in the certification authority, unless he does not exercise control over the certification authority.

3. The notification required in relation to paragraph (1)(*b*) shall be in such form as the Controller may require and shall include the following information:
    - the name of the person with a controlling interest; and
    - the percentage of the voting shares in the certification authority acquired by that person.

REQUIREMENTS FOR REPOSITORY

Regulation 25 - Availability of General Purpose Repository

1. A general purpose repository shall be available at all times of the day and on all days of every year.

2. A general purpose repository must ensure that the total aggregate period of any down time in any period of one month shall not exceed 0.5% of the period.

3. Any down time, whether scheduled or unscheduled, shall not exceed 120 minutes duration at any one time.

Regulation 26 - Specific Purpose Repository

1. Subject to the approval of the Controller, a repository may be dedicated for a specific purpose for which specific hours of operation may be acceptable.

ACCREDITATION MARK

Regulation 27 - Use of Accreditation Mark

1. Any person who, not being an accredited certification authority, uses an accreditation mark or a colourable imitation thereof shall be guilty of an offence and shall be liable on conviction to a fine not exceeding N500,000 or to imprisonment for a term not exceeding 12 months or to both.

APPLICATION TO PUBLIC AGENCIES

Regulation 28 - Application to Public Agencies

1. A public agency that is approved by the Controller to act as a certification authority shall comply with the provisions of these Regulations as if it were an accredited certification authority.

2. The provisions referred to in paragraph (1) shall apply, with the necessary modifications and such other modifications as the Controller may determine, to a public agency referred to in paragraph (1).

ADMINISTRATION

Regulation 29 - Waiver

1. Any accredited certification authority that wishes to apply for a waiver of any of the requirements specified in these Regulations may apply in writing to the Controller at the time when it submits an application for accreditation.

2. The application must be supported by reasons for the application and include such supporting documents as the Controller may require.

Regulation 30 - Disclosure

1. The accredited certification authority must submit half-yearly progress and financial reports to the Controller.

2. The half-yearly progress reports must include information on:
    - the number of subscribers;
    - the number of certificates issued, suspended, revoked, expired and renewed;
    - system performance including system up and down time and any extraordinary incidents;
    - changes in the organizational structure of the certification authority;
    - changes since the preceding progress report was submitted or since the application for the accreditation; and
    - changes in the particulars of any trusted person since the last submission to the Controller, including the name, identification number, residential address, designation, function and date of employment of the trusted person.

3. The accredited certification authority has a continuing obligation to disclose to the Controller any changes in the information submitted.

4. All current versions of the accredited certification authority's applicable certification practice statements together with their effective dates must be published in the accredited certification authority's Internet website.

Regulation 31 - Discontinuation of Operations of Certification Authority

1. If an accredited certification authority intends to discontinue its operations, the accredited certification authority may arrange for its subscribers to re-subscribe to another accredited certification authority.

2. The accredited certification authority shall make arrangements for its records and certificates to be archived in a trustworthy manner.

3. If the records are transferred to another accredited certification authority, the transfer must be done in a trustworthy manner.

4. An accredited certification authority shall:
    - give to the Controller written notice of its intention to discontinue its operations not later than 3 months before the discontinuation;
    - give to its subscribers written notice of its intention to discontinue its operations not later than 2 months before the discontinuation; and
    - advertise, in such daily newspapers and in such manner as the Controller may determine, its intention to discontinue its operations not later than 2 months before the discontinuation.

Regulation 32 - Audit

1. The Controller may, by notice in writing, require an accredited certification authority to undergo and pass an audit.

2. The audit referred to in paragraph (1) must be:
    - conducted in accordance with the auditing requirements specified in this regulation; and
    - completed within such time as the Controller may, by notice in writing, specify.

3. The audit must be conducted by a qualified independent audit team approved by the Controller for this purpose comprising of a person who is a Certified Public Accountant and a person who is a Certified Information Systems Auditor and either of whom must possess sufficient knowledge of digital signature and certificates.
4. The firm or company to which the audit team belongs must be independent of the certification authority being audited and must not be a software or hardware vendor that is or has provided services or supplied equipment to the certification authority.

5. Auditing fees shall be borne by the certification authority.

6. A copy of the audit report shall be submitted to the Controller within 4 weeks of the completion of an audit.

Regulation 33 - Penalties

1. Any person who fails, without any reasonable excuse, to comply with these regulation shall be guilty of an offence and shall be liable on conviction to a fine not exceeding N500,000 and, in the case of a second or subsequent conviction, to a fine not exceeding N1,000,000.

Regulation 34 - Composition of Offences

1. Any offence under these Regulations may be compounded by the Controller.

Regulation 35 - Transitional

1. A certification authority which, immediately before the date of operation of these Regulations, was a licensed certification authority under any previous Regulations shall with effect from that date be deemed to be an accredited certification authority under these Regulations.

2. The deemed accreditation under paragraph (1) shall, unless it is suspended or cancelled, and insofar as it is not inconsistent with these Regulations:
   - be subject to the conditions and restrictions imposed on the licence granted under the previous Regulations; and
   - expire on, and be renewable before, the date when the licence granted under the previous Regulations would have expired if these Regulations had not been enacted.

Appendix

AUDIT COMPLIANCE CHECKLIST

Certificate Authority Overall Governance

S/No.	Control Steps	Checks
	Obligations to Subscribers, Relying Party and User Community	
1	**User Community Obligation** The Auditor shall review that the Certification Authority (CA) has informed the User Community of: 1. The CA's procedures for certificate registration, issuance, suspension and revocation; 2. Any *force majeure* that relieves the CA of its duties; 3. The time-intervals between each update and publication of the certificate suspension, revocation and Certification Revocation List (CRL) information; 4. The scope and limitations of the CA's liabilities with respect to the expected reliance to be placed in the information contained in the certificates; 5. The CA's Certificate Practice Statement (CPS) and Certificate Policies (CP). In addition, the Auditor shall review that: 1. The mode of communication should be reasonable to reach a majority of the User Community; 2. All updates are within the established time-intervals defined by the CA.	1. Sight evidence that the CA has performed its obligation to the User Community as defined in the Control Step
2	**Subscribers Obligation** The Auditor shall review that the CA has informed the Subscribers of their responsibility to validate the accuracy of the information contained in their certificates upon issuance. In addition, the Auditor shall review that: 1. Subscribers' explicit consent has been obtained before publication of their certificates on the repository; 2. The CA has informed the Subscribers on how the private keys have been protected.	1. Sight evidence that the CA has performed its obligation to the Subscribers as defined in the Control Step; 2. Sampled observations of Subscribers' acknowledgements on their responsibility; 3. Inquire the CA if any Subscribers' certificates are published and sight obtained consent.

S/No.	Control Steps	Checks
3	**Relying Party Obligation** The Auditor shall review that the CA has informed the Relying Party on steps to be taken to verify the authenticity and validity of a certificate. The steps shall include but are not limited to the verification of: 1. Issuer's signature; 2. Policy parameters; 3. Usage parameters; 4. Validity period; 5. Revocation or suspension information; and 6. Reliance limit.	1. Sight evidence that the CA has performed its obligation to the Relying Party as defined in the Control Step
Certificate Practice Statement (CPS) and Certificate Policies (CP)		
4	The Auditor shall review that the CA has prepared its CP and CPS using guidelines stated in IETF's *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* (RFC 3647).	1. Inquire the CA on how they prepared the CP and CPS using RFC3647 as guidelines
5	The Auditor shall review that the CP and CPS include the following: 1. Effective date; 2. Version number; 3. Change history; 4. Publication & Repository responsibilities; 5. CA's identification and authentication processes; 6. CA's Certificate Life-Cycle Operations; 7. Physical controls; 8. Procedural controls; 9. Personnel controls; 10. Technical security controls; 11. Audit trails; 12. Certificate and CRL profiles; 13. CA's self-assessment and external audit requirements; 14. Business and Legal matters; 15. Limited liability clauses. In addition, the Auditor shall review that each CP has been defined for each class of certificates. It is possible that all classes of certificates use the same CP.	1. Sight that the CP and CPS minimally contain the information as defined in the Control Step; 2. Sight that each CP has been defined for each class of certificate.
Security Management		
6	The Auditor shall review that regular updates on security risks and exposures are communicated to personnel directly involved in the CA operations. The regular updates can be in the form of email, circulars, website updates or training.	1. Sampled observations of security risks and exposure updates communiqué

S/No.	Control Steps	Checks
7	The Auditor shall review that IT Security Policy exists and: • Is approved by the CA's management; • Is reviewed regularly; • Is communicated to, understood and acknowledged by personnel directly involved in the CA operations.	1. Sight the existence of an IT Security Policy; 2. Sight evidence that the IT Security Policy is approved and reviewed yearly; 3. Sampled observations of personnel acknowledgement forms which indicate they have read and understood the IT Security Policy.
8	The Auditor shall review that personnel responsible for security management have been trained by: 1. Inspecting qualifications/certifications such as CISSP or equivalent; OR 2. Inspecting if the personnel have attended training and the content of the training	1. Observation of training records or certifications
9	The Auditor shall review the access control matrixes and its follow-up actions on a regular basis	1. Observation of monthly access control matrix review reports; 2. Sampled observations which indicate follow-up actions are implemented within 24 hours
10	The Auditor shall review the existence and implementation of: 1. Vulnerability management procedures covering, but not limited to: a. sources of information; b. planning and execution of counter measures. 2. Incident management procedures covering, but not limited to: a. compromise of key; b. penetration of systems or network; c. unavailability of network; d. security incidents; e. fraudulent activities surrounding the registration, generation, suspension and revocation of certificates; f. informing the Controller within 24 hours of any incidents. In addition, the Auditor shall review that the CA has documented and acted on identified incidents.	1. Sight the existence of vulnerability management procedures and that they minimally contain the information as defined in the Control Step. 2. Sampled observations that the vulnerability management procedures are tested and reviewed at least once every 6 months. 3. Sight the existence of incident management procedures and that they minimally contain the information as defined in the Control Step. 4. Sampled observations that the incident management procedures are tested and reviewed every 6 months.

S/No.	Control Steps	Checks
	Risk Management	
11	The Auditor shall review that the CA performs a regular risk assessment of its CA infrastructure, which includes: 1. Cryptographic algorithm and key parameters; 2. Physical security; 3. Operating system security; 4. Network security; 5. Application security; 6. PKI software	1. Observation of risk assessment reports and that the assessment minimally covers the areas as defined. 2. Sampled observations that follow-up actions are implemented within 1 month; 3. Sight evidence that assessment is performed at least yearly or after major changes to CA infrastructure .
12	The Auditor shall review that the CA has the following: 1. Risk Management Policy; 2. Risk Management Procedures. In addition, the Auditor shall review that the CA management review, update and approve the policy and procedures regularly.	1. Sight the existence of Risk Management Policy and Procedures; 2. Sight evidence that the IT Risk Management Policy is reviewed, updated and approved yearly; 3. Sight evidence that the IT Risk Management Procedures are reviewed, updated and approved half-yearly
	Personnel Controls	
13	The Auditor shall review that the CA has taken steps to verify that personnel to be employed for direct CA operations are subject to security screening. The security screening should cover: 1. Criminal history; 2. Bankruptcy status; AND 1. Personnel self-declaration on criminal and bankruptcy history. In addition, the Auditor shall review that the CA performs regular reviews of the security screening of personnel.	1. Sight security screening process documentation that the security screening minimally covers the areas as defined in the Control Step; 2. Sampled observations of security screening documents; 3. Sampled observations of personnel self declaration forms.
14	The Auditor shall review that the CA implements dual control to: 1. Root equivalent accounts to systems; 2. Administrative accounts to key applications.	1. Sight access matrix that personnel assigned to root accounts and administrative accounts have dual controls

S/No.	Control Steps	Checks
15	The Auditor shall review that: 1. All personnel involved in CA operations have signed a confidentiality agreement; 2. These confidentiality agreements are reviewed when the terms of their employment contracts change.	1. Sampled observations of confidentiality agreements; 2. Sampled observations that confidentiality agreements are reviewed during employment contract changes (hires and terminations).
16	The Auditor shall review that the CA has documented and implemented segregation of duties for key CA operational roles, including but not limited to: 1. Requestor – Approval; 2. Maker – Checker; 3. Administration – Security; 4. Operations – Security.	1. Sight access control matrixes that conflicting roles are not present; 2. Observation that system access controls are according to segregation of duties.
17	The Auditor shall review that the CA designs and implements job responsibilities and the corresponding access matrix (logical and physical). The job responsibilities and access matrix should be documented and contain: 1. Effective date and validity; 2. Role description and assignees; 3. Access control assigned (including physical security); 4. Training requirements. The job responsibilities and access matrix should include names of backups. In addition, the Auditor shall review that the CA reviews the job responsibilities and access matrix regularly.	1. Sight access control matrix that it minimally covers the areas as defined in the Control Step; 2. Sample observations that job responsibilities and access matrix are reviewed at least once every 3 months; 3. Observation that system access controls are according to assigned responsibilities
	Subscriber's Data	
18	The Auditor shall review that the CA has designed and implemented steps to protect the confidentiality and privacy of the Subscribers' data, including transactional and historical data about the Subscribers' usage.	1. Sight the existence of procedures surrounding protection of Subscribers' data; 2. Sampled observations of protection mechanism.
19	The Auditor shall review that explicit permissions have been obtained from the Subscribers by the CA for third party disclosure.	1. Sampled observations of permissions obtained from Subscribers for third party disclosure
	Incident Management	
20	The Auditor shall review that the CA has an approved Incident Management Plan. The Plan should include, but is not limited to the following: 1. Key compromise (RA Key, CA certification Key); 2. Intrusion to systems and network;	1. Sight existence of an Incident Management Plan that minimally covers the areas as defined in the Control Step;

	3. Breach of physical security; 4. Infrastructure downtime; 5. Fraudulent activities surrounding certificate management. The Auditor shall also review that the CA has informed the Controller promptly for **confirmed** incidents	2. Sampled observations that the CA has informed the Controller within 24 hours for confirmed incidents.
21	The Auditor shall review that the CA has an approved Incident Response Action Plan. The Plan should include, but is not limited to the following: 1. Compromise control; 2. Revocation conditions and procedures(e.g. revocation of CA certificate in the event that the CA certification key is lost or compromised); 3. Notification Parties and procedures; 4. Service disruption procedures; 5. Audit trail protection and analysis; 6. Media and public relations. The Auditor shall review that the CA has tested and trained personnel on usage of the Incident Response Action Plan.	1. Sight existence of an Incident Response Action Plan that minimally covers the areas as defined in the Control Step; 2. Sight evidence that the key personnel were trained on the Plan; 3. Sight evidence that the Plan is tested at least annually; 4. Sampled observations that the Plan is used for actual incidents
	Business Continuity Planning	
22	The Auditor shall review that the CA has the following plans available: 1. Business Continuity Plans; 2. Disaster Recovery (DR) Plans. The Plans should include: 1. Continuity plans in the event of CA certification key loss or compromise; 2. Named personnel in the recovery team; 3. The availability of cold backups (redundant systems); 4. Location of the DR site; 5. Backup procedures for use in the event of *force majeure* not being excluded from their obligations. In addition, the Auditor shall review that the Plans have been tested and inadequacies were rectified	1. Sight existence of a Business Continuity Plan that minimally covers the areas as defined in 2. the Control Step; 3. Sight existence of a Disaster Recovery Plan that minimally covers the areas as defined in the Control Step; 4. Sampled observations that Plans are tested and reviewed at least once every 6 months; 5. Sample observations that inadequacies in the Plans are rectified.
23	The Auditor shall review that the named personnel in the recovery team have been trained in the execution of the Plans.	1. Sampled observations of Plan training records of recovery team.
24	The Auditor shall review that the cold backups of the hardware used in the Plans are available and accessible.	1. Sight sampled cold backups can be started.
25	The Auditor shall review that the DR site has basic security (physical and environmental) in place.	1. Inquire the CA on security controls in place at DR site; 2. Sampled observations of security controls in DR site.

Certificate Management Controls

S/No.	Control Steps	Checks
26	The Auditor shall review that the following exists as certificate attributes: 1. Certificate policy; 2. Usage parameters; 3. Expiration parameters; 4. Distinction between CA certificate and user certificate. In addition, the Auditor shall review that the following information do not exist: 1. Distinguished name fields; 2. 2. Other information of users that may be used in social engineering.	1. Observation of sampled certificates that have certificate attributes as defined in the Control Step
	Registration Process	
27	The Auditor shall review that the CA has defined and implemented authentication methods to verify the certificate applicant. The Auditor shall also review that the authentication documents used are retained.	1. Sight authentication procedures; 2. Sample certificates issued by the CA and sight corresponding authentication documents.
	Generation Process	
28	The Auditor shall review that the procedures adhered to in the generation process are in accordance to the CP.	Sampled observations of evidence that the generation process is carried out in accordance to the CP.
29	The Auditor shall review that the: 1. Information in the certificate is the same as in the request; 2. The correct key pair is associated with the certificate information	1. Sampled comparisons that request information is the same as in the generated certificates; 2. Sight evidence that the correct key pair is associated with the certificate information
	Issuance Process	
30	The Auditor shall review that the issuance channel used for the transmission of certificate, passwords and private keys between the CA and Subscribers is secure. In addition, the Auditor shall review that receipt of certificates is acknowledged and accepted by the Subscribers.	1. Inquire the CA on protection mechanisms used for the transmission of certificates; 2. Sampled observations of the implemented protection mechanisms; 3. Sampled observations of acknowledgements of receipt and acceptance by Subscribers

S/No.	Control Steps	Checks
	Publication Process	
31	The Auditor shall review that the CA has published its certificate, CP, CPS and repository in a secure channel. In addition, the Auditor shall review that the following information is available for the User Community to verify: 1. Company Name; 2. Registration number; 3. X500 name; 4. Internet address; 5. Telephone number; 6. CA certificate; 1. 7. Location of repository.	1. Inquire the CA on protection mechanisms used for publication; 2. Sampled observations of the implemented protection mechanisms; 3. Sight that the information is available for the User Community and minimally contains the information defined in the Control Step.
32	The Auditor shall review that the CA obtained explicit consent for publication of Subscriber's certificate information.	1. Sampled observations of consent given for certificate information that was published
33	The Auditor shall review that access to the repository: 1. Is read-only to the public, Subscribers and User community; 2. Has restricted access to the CA's assigned personnel for updating the repository. In addition, the Auditor shall review that the modifications to the CPS are subject to a change management procedure of request and approval.	1. Inquire the CA on access controls to the repository; 2. Sampled observations of the implemented access controls; 3. Sampled observations of change management request and approval forms.
	Renewal Process	
34	The Auditor shall review that the renewal requests are submitted using a secure channel OR using the same authentication method in the registration process.	1. Observation of security mechanism of renewal; 2. Inspection of sampled renewal requests for evidence that the secure renewal channel is used.
	Certificate Suspension Process	
35	The Auditor shall review that suspended certificates are reactivated by the CA after investigations have completed and no compromise has been confirmed.	1. Sampled observations of reactivated certificates have supporting documents that indicate no compromise.
36	The Auditor shall review that the CA has taken steps to verify the identity of the requestor of certificate suspension.	1. Sampled observations of identity verification documents
37	The Auditor shall review that the CA has taken steps to ensure that the suspension information in the CRL is protected from unauthorized modifications	1. Inquire the CA on protection mechanisms used to prevent unauthorized modifications of suspension information; 2. Sampled observations of the protection method ..

S/No.	Control Steps	Checks
38	The Auditor shall review that the CA has informed the Subscriber of suspension.	1. Sampled observations of communication to Subscribers.
39	The Auditor shall review that information of suspended certificates are updated in the CRL and are digitally signed by the CA.	1. Sight evidence that the CRL is updated within 1 hour upon verification that suspension request is valid; 2. Sight updates include reason and date/time of suspension; 3. Sight all updates are digitally signed by the CA.
	Revocation Process	
40	The Auditor shall review that the CA revokes the certificate when: 1. Information marked with extension "critical" is inaccurate; 2. Private key or media holding the private key is suspected or actually compromised; 3. Subscriber is no longer a member of the community subject to CP; 4. The Subscriber requests it; 5. Suspected or actual violations of the generation or issuance process; 6. CA certificate is compromised	1. Sight revocation procedures cover the conditions described in the Control Step; 2. Sampled observations of incidents which meet revocation conditions are revoked.
41	The Auditor shall review that the CA has taken steps to verify the identity of the requestor of certificate revocation.	1. Sight the CA verification procedures; 2. Sampled observations of verification documents
42	The Auditor shall review the certificate revocation information contain, but is not limited to the following: 1. Reason for revocation; 2. Revocation date/time. In addition, the Auditor shall review that the certificate revocation information is digitally signed and published by the CA.	1. Sampled observations of certification revocation information as described in the Control Step; 2. Sampled observations that the revocation information is digitally signed by the CA; 3. Sampled observations that the revocation information is published.
43	The Auditor shall review that the CA has taken steps to ensure that the certificate revocation information is protected from unauthorized modifications.	1. Inquire the CA on protection mechanisms used to prevent unauthorized modifications of revocation information; 2. Sampled observations of the protection mechanisms

S/No.	Control Steps	Checks
44	The Auditor shall review that the CA has informed the Subscriber of revoked certificates.	1. Sampled observations of communication that the CA has informed the Subscriber of revoked certificates within 1 hour.
45	The Auditor shall review that the CA do not re-activate revoked certificates	1. Inquire the CA on measures taken to prevent the reactivation of revoked certificates; 2. Sampled observations of the measures.
	Archival Process	
46	The Auditor shall review that all certificate suspension and revocation information, certificates, registration documents are archived for 7 years.	1. Sampled observations of archived information (one for each year).
47	The Auditor shall review that the CA tests the archival process for accuracy, security and accessibility for digital archives.	1. Sight test results; 2. Sight evidence that testing is performed at least yearly; 3. Sampled observations that negative testing has been rectified.
	Audit Trails	
48	The Auditor shall review that the CA keeps audit trails of certificate registration, generation, issuance, renewal, suspension and revocation.	1. Inquire the CA on the audit trails kept; 2. Sampled observations of the audit trails.
49	The Auditor shall review the security mechanism the CA implements for the protection of audit trails.	1. Inquire the security mechanisms used to protect the audit trails; 2. Sampled observations of the security mechanisms.
50	The Auditor shall review that the CA conducts periodic reviews of the audit trails.	1. Sight audit review documents; 2. Sight evidence that audit trails are reviewed at least once every 2 days.
51	The Auditor shall review that the CA keeps audit trails for 12 months.	Sampled observations of audit trails (sampled for each month).

Key Managemnt Controls

S/No.	Control Steps	Checks
	Generation	
52	The Auditor shall review that segregation of duties exists between personnel involved in system setup and maintenance and personnel involved in the key generation process. In addition, the Auditor shall also review that keys are stored under dual control.	1. Sight access control matrixes that conflicting roles are not present and dual control exists for key assignment; 2. Observation that system access controls are according to segregation of duties
53	The Auditor shall review that separate key pairs exists for digital signature and encryption.	1. Observation of separate key pairs.
54	The Auditor shall review that the CA uses random key values in the generation of keys. The Auditor shall also review that the seed (input) used in the random generator is not static and not predictable	1. Inquire the CA on how seeds are produced; 2. Sampled observations of seed generation
55	The Auditor shall review that the CA provides reviews and approves the key generation system used by the Subscribers	1. Sampled observations of approval of key generation system used by the Subscribers
	Distribution	
56	The Auditor shall review that the CA has prescribed procedures for transferring the keys from the key generation system to the storage device in a secure manner.	1. Inquire the CA on protection mechanism of transferring keys; 2. Sampled observations of the protection mechanism.
	Storage	
57	The Auditor shall review the CA has provided Subscribers the necessary instructions and programs to safeguard and encrypt the Subscribers' private keys.	1. Sight instructions and programs to Subscribers
58	The Auditor shall review that the CA stores its keys in tamper proof devices. In addition, the Auditor shall review that: 1. Access to the tamper proof devices is dual controlled by personnel not involved in the setup, maintenance and operations of the CA systems; 2. The CA documents and approves the change of key custodians; 3. Backup custodians to reduce key-man risks exist.	1. Observation of tamper proof devices; 2. Sampled observations of key custodian change documentation; 3. Sight access control matrixes for key custodians, backups and segregation of duties of custodians.
	Backups	
59	The Auditor shall review that the CA stores its backup keys in a separate physical location as the original key.	1. Observe separate physical location for backup keys

S/No.	Control Steps	Checks
60	The Auditor shall review that the CA private keys are backed up.	1. Observation of the backup private keys; 2. Sight evidence that the backup keys are subject to the same controls as the original keys.
	Usage	
61	The Auditor shall review that the CA implements dual control loading of the certificates. In addition, the Auditor shall review that the CA performs integrity checks prior to loading of the certificates.	1. Inquire the CA on procedures of dual control on loading of certificates; 2. Inquire the CA on integrity checks; 3. Sampled observations that integrity checks and dual control are implemented
	Key Change	
62	The Auditor shall review that the CA change the CA and Subscriber keys periodically. In addition, the Auditor shall review that the CA has provided notice to: 1. The Subscribers' relying parties of new key pairs used to sign certificates; 2. The Subscriber or owner of changed key in a secured manner.	1. Sampled observations of key change documentation; 2. Sampled observations that the CA has provided notice to the Subscriber as defined in the Control Step.
63	The Auditor shall review that the CA has a key interlock procedure and implements the procedure during key change.	1. Sight the key interlock procedures; 2. Sampled observations that procedures were followed.
	Destruction	
64	The Auditor shall review that the CA archives and securely stores the backup copies upon the termination of a CA signature private key	1. Sampled observations of archives and backups
	Key Archival	
65	The Auditor shall review that the CA has archived: 1. All CA Public keys (permanently) 2. All Subscriber encryption keys.	1. Sampled observations of archives
66	The Auditor shall review that the archives are protected from unauthorized modification	1. Inquire the CA of the protection mechanisms; 2. Sampled observations of the protection mechanism having been implemented
	Key Compromise	
67	The Auditor shall review that the CA has revoked all affected Subscriber certificates in the event of CA certification private key compromise	1. Inquire the CA of historical compromise; 2. Observe affected certificates are revoked

S/No.	Control Steps	Checks
68	The Auditor shall review that the CA has an escalation process in the event of suspected or actual key compromise. In addition, the Auditor should review that the Controller is informed within 24 hours of suspected or actual key compromise.	1. Inquire the CA of historical compromise; 2. Sample compromise events and sight for evidence that the CA has informed the Controller within 24 hours.
69	The Auditor shall review that the CA has revoked all affected keys and certificates in the case of subscriber private key compromise	1. Inquire the CA of historical compromise; 2. Observation that affected keys and certificates have been revoked..
	Cryptographic Engineering	
70	The Auditor shall review that the CA performs its cryptographic processes in a hardware cryptographic module that minimally conforms to: 1. FIPS 140-1 Security Level 3; 2. FIPS 140-2 Security Level 3. For Registration Authority (RA) operations away from the CA, the cryptographic module should minimally conform to: 1. FIPS 140-1 Security Level 2; 2. FIPS 140-2 Security Level 2.	1. Sight evidence that the cryptographic hardware used has the appropriate FIPS certification
71	The Auditor shall review that the CA has communicated to its Subscribers that their cryptographic operation should conform minimally to: 1. FIPS 140-1 Security Level 1; 2. FIPS 140-2 Security Level 1.	1. Sampled observations of communication to Subscribers and that it contains the minimum requirement of FIPS compliance
72	The Auditor shall review that the CA ensures: 1. Cryptographic keys and algorithms are sufficient to protect the cryptographic results; 2. Asymmetric cryptographic algorithms conform to the IEEE standard specifications	1. Inquire the CA on the sufficiency testing of the cryptographic keys and algorithms; 2. Sight evidence that the asymmetric cryptographic algorithms used are IEEE compliant.

System and Operational Controls

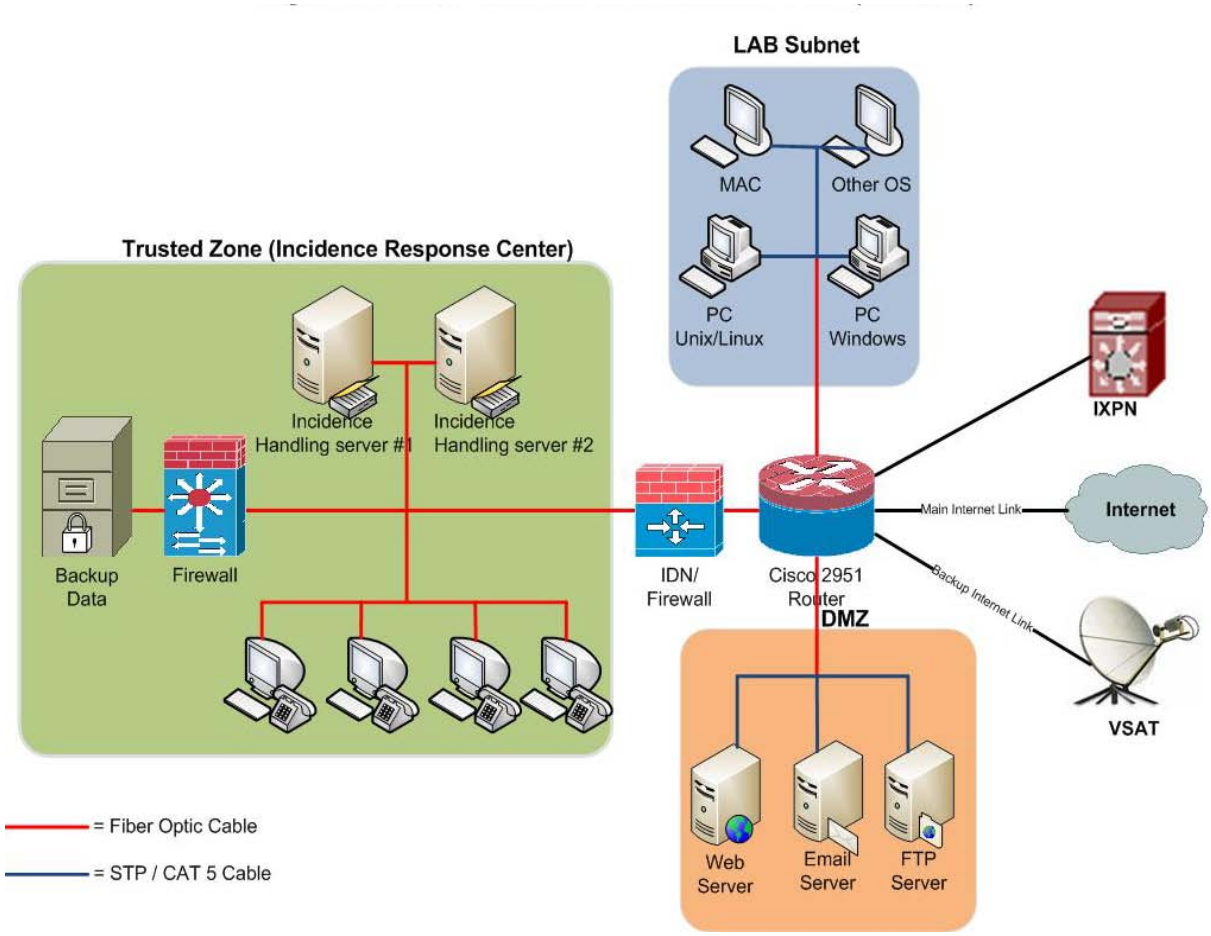
S/No.	Control Steps	Checks
73	The Auditor shall review that access control matrixes physical and logical) are defined for all operating systems, network devices, applications and databases used in the CA operations exist. The access control matrixes should include, but are not limited to: 1. Personnel names; 2. Access granted; 3. Validity of access rights; 4. The next access control matrix review date. In addition, the Auditor shall review the application and currency of the access controls defined in the access control matrixes.	1. Sight access control matrix minimally covers the areas as defined in the Control Step; 2. Observation of system, network, application and database access controls are implemented in accordance to the access control matrix
74	The Auditor shall review that the CA performs an assessment of the CA infrastructure components, which includes: 1. Operating system; 2. Network devices; 3. Security software (e.g. Intrusion Detection System and Antivirus Software). A full assessment is required for new components and an incremental assessment is required for updates or modifications to the infrastructure.	1. Sight assessment report and follow-up actions. 2. Sampled observations that follow-up actions are implemented
75	The Auditor shall review that the CA performs regular scans using tools of its systems and network devices to identify security vulnerabilities. The tools must be able to scan system and network vulnerabilities. In addition, the Auditor shall review that follow-up actions have been performed.	1. Sampled observations of scan results; 2. Sight evidence that scanning is performed at least once a eek; 3. Sampled observations that follow-up actions are implemented.
76	The Auditor shall review that the CA has deployed Intrusion Detection System (IDS). In addition, the Auditor shall review that follow-up actions have been performed for potential intrusions.	1. Sampled observations of follow-up actions of detected intrusions; 2. Sight evidence that the IDS covers 100% of components of the CA infrastructure
77	The Auditor shall review that the CA performs regular log review of the following (using the access control matrixes): 1. Unauthorized access and modifications to key system files and utilities; 2. Unauthorized access and modifications of Subscribers' data.	1. Observation of log review reports 2. Sampled observations that follow-up actions have been implemented

S/No.	Control Steps	Checks
	Physical Security	
78	The Auditor shall review that: 1. The location of the CA system is not publicly identified; 2. Physical security systems are installed; 3. Inventory of access control cards are dual-controlled; 4. Loss of access control cards are reported and follow-up 1. actions are performed; 5. Systems performing certification should be partitioned under lock and key; 6. Entry to the partition must be logged with timestamps; 7. Entry logs are reviewed: 8. Access to infrastructure components (power control, communication riders and cabling) is restricted to authorized personnel; 9. An approval process for temporal or bypass access exists; 10. An IDS exists.	1. Sampled observations that the CA carries out the items described in the Control Step; 2. Sight evidence that entry logs are reviewed daily.
	General Security Controls	
79	The Auditor shall review that: 1. Systems performing certification functions are not used for general purposes (e.g. word processing, emailing, web surfing); 2. Strong password policies are implemented; 3. System administrators are trained; 4. CA application operators are trained; 5. Inactive lockouts are implemented (no longer than 10 minutes of inactivity before lockout); 6. Updated security patches are reviewed, tested, applied and implemented.	1. Sampled observations that the CA carries out the items described in the Control Step
	Network Security	
80	The Auditor shall review that: 1. Network access control exists to separate and isolate CA systems from the other systems; 2. Communications between CA systems should be secure and data should not be transmitted in the clear; 3. IDS is present and that the IDS monitors the CA systems.	1. Sampled observations that the CA carries out the items described in the Control Step
	General Operational Controls	
81	The Auditor shall review that: 1. System administrators are trained; 2. CA application operators are trained.	1. Sampled observations of training records.

S/No.	Control Steps	Checks
	Change and Configuration Management	
82	The Auditor shall review that: 1. All changes are supported by change requests; 2. All change requests are approved before construction; 3. All source codes should be version-controlled; 4. There is an approved process of moving from development to production; 5. Segregation of duties exists for source code migration.	1. Sampled observations that the CA carries out the items described in the Control Step.
	Monitoring and Audit Trails	
83	The Auditor shall review that the CA has the following audit trails: 1. Application transactions: a. Registration; b. Certification; c. Publication; d. Suspension; and e. Revocation. 2. System log files: a. Security violations; b. Errors; c. Execution of privilege functions; d. Changes in access control and system configurations. n addition, the Auditor shall review that the: 1. audit trails are protected from unauthorized access; 2. and retained for a minimum period of 12 months	1. Sampled observations of audit trails and that they cover the items described in the Control Step; 2. Inquire the CA on the protection mechanism of audit trails; 3. Sampled observations of the protection mechanism; 4. Sampled observations of audit trail retention (sample from each month).
84	The Auditor shall review that the CA performs regular reviews of the audit trails and follow-up actions are performed.	1. Observation of audit trail review reports; 2. Sampled observations that follow-up actions have been implemented

Application Integration Controls		
S/No.	**Control Steps**	**Checks**
85	The Auditor shall review that the application toolkits provided by the CA to the user and developer community comply with the following: 1. The user shall be informed when a private key is being accessed; 2. The user shall be alerted if its private key is being used for a purpose that is not consistent with that defined as acceptable use by the issuer; 3. Mechanisms shall be available to check the integrity of the applications for unauthorised modifications, especially the integrity of signing and verification functions; 4. Application security risk assessment on the CA's software infrastructure should be conducted yearly to ensure that the CA's software that manages, issues and revokes certificates is developed to manage the risk identified; 5. The application should securely purge the private key temporarily stored for processing to minimise private key exposure; 6. The application shall verify the validity and authenticity of the certificate; 7. The verification process shall trace and verify all the components in the certification path; 8. For validity and authenticity verification, it shall be necessary to verify that: a. The certificate issuer's signature is valid; b. The certificate is valid (i.e. has not expired, been suspended or revoked); and c. The certificate extensions flagged as "critical" are being complied with.	1. Sight that each application toolkit provided by the CA minimally complied with the requirements as defined in the Control Step

Sample PKI Network Infrastructure



References

- BS 7799-12000 – General IT Systems and Operations
- BS 7799-12000 – Code of Practice for Information Security Management
- NIST - Information Processing Standard
- IEEE PI363 – Standard Specifications for PKI
- ITU Recommendations for X.509 Certificate Format