

THE LICENCE TERMS

The Communications Authority of Kenya (hereinafter referred to as the “Authority”), in accordance with the Kenya Information & Communications Act, Cap 411A (hereinafter referred to as the “Act”), hereby authorises “**the Licensee**” to establish and provide electronic certification services “**Licensed Services**” in the Republic of Kenya in accordance with the Terms and Conditions set out in this license.

1. This Licence is granted for a period of fifteen (15) years (the “**Licence Period**”) from the Effective Date unless it is revoked earlier in accordance with the Licence Conditions herein.
2. The Licensee is authorised to provide Electronic Certification Services. Electronic Certification Services” means issuance and renewal of electronic certificates; suspension, reinstating or revocation of certificates; conducting personal identification of subscribers; publishing accurate information related to certificates; providing a repository service, listing all published certificates, records of revoked certificates that may be used to verify the validity of published certificates; ensuring protection of private information and safe keeping data security; and providing time stamp services; .
3. The Electronic Certification Services shall be accessed by means of facilities of licensed Network Facilities Providers and/or services of licensed Application Service Providers.
4. The Licensee is authorised to provide the Licensed Services provided that:
 - 4.1. The Licensee has obtained accreditation from the Authority and/or the related authorisations from Governmental Authorities and such an authorisation has been filed with the Authority;
 - 4.2. the Licensee has filed the details of the service to be provided and obtained approval from the Authority; and
 - 4.3. a separate licence is not required to provide the service.
5. All equipment and devices used to provide the Licensed Services shall in all respects be of an approved industrial standard, type approved by the Authority and conforming to the Authority’s regulations as may be issued from time to time.
6. This Licence is subject to the provisions of the Act including, but not limited to, licence modifications and enforcements.

7. Words importing the singular shall include the plural and vice versa; words denoting persons shall include bodies corporate and unincorporated associations of persons and vice versa.
8. In this Licence the following terms shall have the following meanings:
- 8.1. **“Act”** means the Kenya Communications Act 1998, any successor legislation and any subsequent amendments made thereto;
- 8.2. **“Accreditation”** – means attestation by the Authority that an Electronic Certification Service Provider is competent to carry out Electronic Certification Services.
- 8.3. **“advanced electronic signature”** means an electronic signature which meets all the following requirements:
- a) is uniquely linked to the signatory;
 - b) can identify the signatory;
 - c) it is created using means that the signatory can maintain under his sole control; and
 - d) it is linked to the data to which it relates in such a manner that any subsequent change to the data is detectable;
- 8.4. **“Application Services”** means electronic communications services which are normally provided for remuneration and consists wholly or mainly in the conveyance of signals on electronic communications networks including telecommunications and transmission services over electronic communications networks including those used for broadcasting, but exclude services providing or exercising editorial control over, content transmitted using electronic communications networks and services;
- 8.5. **“Application Service Provider (ASP)”** means a licensee authorised by the Authority to provide Application Services;
- 8.6. **“Certificate”** means a record which is issued by a certification service provider 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; identifies the certification service provider issuing it; names or identifies the person to whom it is issued; contains the public key of the person to whom it is issued; and is signed by a responsible officer of the certification service provider issuing it;

- 8.7. **“Compliance Report”** means a report to be prepared periodically by the Licensee detailing its performance in respect of every licence condition;
- 8.8. **“Compliance Certificate”** means a certificate to be issued by the Authority to a licensee following the receipt and satisfactory review of a Compliance Report;
- 8.9. **“Electronic Certification Services”** means issuance and renewal of certificates; suspension, reinstating or revocation of certificates; conducting personal identification of subscribers; publishing accurate information related to certificates; providing a repository service, listing all published certificates, records of revoked certificates that may be used to verify the validity of published certificates; ensuring protection of private information and safe keeping data security; and providing time stamp services;
- 8.10. **“Electronic Certification Service Provider (E-CSP)”** referred to as “certification service provider” in the Act means a person authorised by the Authority to provide electronic certification services;
- 8.11. **“Consumer”** means any natural person or legal entity who uses or requests a publicly available electronic certification service.
- 8.12. **“Effective Date”** means the date when the Licence was first issued, or in the case of a Licence replacement, the date when the original Licence was issued;
- 8.13. **“electronic”** means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities;
- 8.14. **“electronic form”** with reference to information, means any information generated, sent, received or stored in magnetic, optical, computer memory, microfilm or similar device;
- 8.15. **“electronic signature”** means data in electronic form affixed to or logically associated with other electronic data which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message;
- 8.16. **“Government”** means the Government of the Republic of Kenya;
- 8.17. **“Network Facilities Provider (NFP)”** means a licensee authorised by the Authority to build and commercially operate Telecommunication/electronic communications Systems;

- 8.18. **“Public Key Infrastructure (PKI)”** means the whole system of policies, processes and technologies including digital certificates, certificate servers and Certification Authorities (CAs) working together to enable users to exchange information over open networks securely and confidentially
- 8.19. **“Regulations”** means the Kenya Communications Regulations, 2001 and its subsequent amendments;
- 8.20. **“Service Level Agreement”** means an agreement entered between the Licensee and a Subscriber defining the nature of the services to be provided and establishing a set of parameters to be used in measuring the agreed service level;
- 8.21. **“Subscriber”** means any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic certification services for the supply of such services;
- 8.22. **“Tier”** is used to distinguish the scope of the various NFP licences. The Authority shall, from time to time, define the various Tiers;
- 8.23. **“User”** means a natural person or legal entity using or requesting a publicly available electronic certification service;
- 8.24. **“X.500 name”** means a name based on a computer network standard that defines directory services

THE LICENCE CONDITIONS

1. CONDITION 1: PROVISION OF LICENSED SERVICES

- 1.1. The Licensee shall meet the rollout requirements set out in Annex 1 of this Licence (the “Rollout Requirements”) and as reviewed by the Authority every five years thereafter.
- 1.2. The Licensee shall provide the Licensed Services to any person on reasonable request.
- 1.3. The obligation in 1.2 shall not apply in the event that it is not, in the Authority's view, reasonable to require the Licensee to comply with such an obligation in the particular circumstances, including, but not limited to circumstances:
 - 1.3.1. where the provision of the service would expose any person engaged in its provision to undue risk to health or safety, and
 - 1.3.2. where it is not reasonably practicable (including where the Licensee is not in a position to provide the requested service in a particular area by reason of the fact that the required electronic certification systems are not sufficiently built out).
- 1.4. The Licensee shall be liable to pay such penalties as set out in Annex 2 for failure to meet the Rollout Requirements in 1.1.

2. CONDITION 2: ACCREDITATION OF ELECTRONIC CERTIFICATION SERVICE PROVIDER

Following the issuance of a license:

- 2.1. The Licensee shall be required to roll out the required infrastructure within a period not exceeding one (1) year;
- 2.2. The Licensee shall apply to the Authority for accreditation;
- 2.3. The Authority shall conduct a compliance audit in order to determine that the licensee meets the requirement for accreditation as per the license conditions;

2.4. Where the Licensee meets the requirements for accreditation, the Authority shall accredit the Licensee to commence operations.

3. CONDITION 3: TECHNICAL REQUIREMENTS

The Licensee shall put in place facilities and equipment for:

- 3.1. Managing the private key and public key.
- 3.2. Managing the registration of user information
- 3.3. Issuance of certificates
- 3.4. Time Stamping
- 3.5. Verification of the online certificate status.
- 3.6. Safe operation of facilities and equipment.
- 3.7. Providing appropriate software to subscribers.

4. CONDITION 4: HUMAN CAPITAL REQUIREMENTS AND CONTROLS

The Licensee shall:

- 4.1. Ensure that operational personnel have at least two (2) years work experience in a field related to Information Security and Management Information Systems.
- 4.2. Take steps to verify that personnel to be employed for its operations are subject to security screening. The security screening should cover: Criminal history; bankruptcy status; and personnel self-declaration on criminal and bankruptcy history.
- 4.3. Perform regular reviews of the security screening of its personnel.
- 4.4. Ensure that all its personnel involved in its operations have signed a confidentiality agreement. These confidentiality agreements shall be reviewed when the terms of the employees' contracts change.
- 4.5. Document and implement segregation of duties for its key operational roles, including but not limited to Requestor vis-à-vis Approver; Maker vis-à-vis Checker; Administration vis-à-vis Security and Operations vis-à-vis Security.

- 4.6. Implement dual control to Root equivalent accounts to systems and Administrative accounts to key applications.
- 4.7. Design and implement job responsibilities and the corresponding access matrix (logical and physical). The job responsibilities and access matrix shall be documented and contain effective date and validity; role description and assignees; access control assigned (including physical security); training requirements and names of backup personnel. These shall be reviewed at least once every three (3) months.

5. CONDITION 5: CONSUMER OBLIGATION

The Licensee shall put in place procedures to inform the Consumers of:

- 5.1. The Licensee's procedures for certificate registration, issuance, suspension and revocation;
- 5.2. Any *force majeure* that relieves the Licensee of its duties;
- 5.3. The time-intervals between each update and publication of the certificate suspension, revocation and Certification Revocation List (CRL) information;
- 5.4. The scope and limitations of the Licensee's liabilities with respect to the expected reliance to be placed in the information contained in the certificates;
- 5.5. The Licensee's Certificate Practice Statement (CPS) and Certificate Policies (CP).
- 5.6. The mode of communication which should be reasonable to reach a majority of the consumers;

6. CONDITION 6: SUBSCRIBERS OBLIGATION

The Licensee shall;

- 6.1. Inform the Subscribers of their responsibility to validate the accuracy of the information contained in their certificates upon issuance.
- 6.2. Obtain explicit consent of the subscribers before publication of their certificates on the repository;

- 6.3. Inform the Subscribers on how the private keys have been protected.

7. CONDITION 7: RELYING PARTY OBLIGATION

The Licensee shall inform 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 issuer's signature; policy parameters; usage parameters; validity period; revocation or suspension information; and, reliance limit.

8. CONDITION 8: CERTIFICATE PRACTICE STATEMENT (CPS) AND CERTIFICATE POLICIES (CP)

The Licensee shall ensure that:

- 8.1. Its CPS and CP are in line with the guidelines in the ITU-T Recommendation (International Standard) X.509 and the Internet Engineering Task Force's (IETF's) *Internet X.509 Public Key Infrastructure 'Certificate Policy and Certification Practices Framework'* (RFC 3647) or later versions.
- 8.2. Its CPS and CP include Effective date, Version number, Change history, Publication & Repository responsibilities, CSP's identification and authentication processes, CSP's Certificate Life-Cycle Operations, Physical controls, Procedural controls, Personnel controls, Technical security controls, Audit trails, Certificate and CRL profiles, CSP's self-assessment and external audit requirements, Business and Legal matters and Limited liability clauses.
- 8.3. That each CP has been defined for each class of certificates. It is possible that all classes of certificates use the same CP.

9. CONDITION 9: SECURITY MANAGEMENT

The Licensee shall:

- 9.1. Ensure that an IT Security Policy is in place and is reviewed annually.
- 9.2. The IT security Policy is communicated to, understood and acknowledged by personnel directly involved in the Licensee's operations.
- 9.3. Ensure that regular updates on security risks and exposures are communicated to personnel directly involved in the Licensee's operations.

The regular updates can be in the form of email, circulars, website updates or training.

- 9.4. Ensure that personnel responsible for security management have been adequately trained.
- 9.5. Ensure that access control matrixes on a monthly basis and its follow-up actions are implemented within 24 hours.
- 9.6. Ensure the existence and implementation of vulnerability management procedures covering, but not limited to sources of information; and planning and execution of counter measures. These procedures shall be tested and reviewed at least once every six (6) months.
- 9.7. Ensure the existence and implementation of incident management procedures covering, but not limited to compromise of key, penetration of systems or network, unavailability of network, security incidents, fraudulent activities surrounding the registration, generation, suspension and revocation of certificates and informing the Authority within 24 hours of any incidents. These procedures shall be tested and reviewed at least once every six (6) months.
- 9.8. Ensure that the identified incidents are documented and acted on.

10. CONDITION 10: RISK MANAGEMENT

The Licensee shall:

- 10.1. Perform regular risk assessment of its infrastructure, which shall include Cryptographic algorithm and key parameters; physical security; operating system security; network security; application security; and Public Key Infrastructure (PKI) software. The Risk assessment shall be performed at least once a year and its follow up actions shall be implemented within one (1) month.
- 10.2. Put in place Risk Management Policy and Risk Management Procedures. The Risk Management policy shall be reviewed at least once a year while the Risk Management Procedures shall be reviewed at least once every six (6) months.

11. CONDITION 11: INCIDENT MANAGEMENT

The Licensee shall:

- 11.1. Put in place an incident management plan that shall include, but is not limited to key compromise; intrusion to systems and network; breach of physical security; Infrastructure downtime; and fraudulent activities surrounding certificate management.
- 11.2. Inform the Authority of any confirmed incidents within twenty four (24) hours.
- 11.3. Put in place an Incident Response Action Plan. The Plan shall include, but is not limited to, compromise control; revocation conditions and procedures (e.g. revocation of its certificate in the event that the Licensee's certification key is lost or compromised); notification parties and procedures; service disruption procedures; audit trail protection and analysis; and media and public relations. The plan shall be tested and personnel trained on usage of the Incident Response Action Plan at least once a year.

12. CONDITION 12: BUSINESS CONTINUITY PLANNING

The Licensee shall:

- 12.1. Put in place a Business Continuity Plan that shall include plans in the event of its certification key loss or compromise; named personnel in the recovery team; the availability of cold backups (redundant systems); location of the Disaster Recovery (DR) site; backup procedures for use in the event of *force majeure* not being excluded from their obligations; and data retention provisions in line with the KICA 411A of 1998. The Plan shall be tested and reviewed at least once every six (6) months and inadequacies rectified within two (2) months.
- 12.2. Ensure that the named personnel in the recovery team have been trained in the execution of the Plans.
- 12.3. Ensure that cold backups of the hardware used in the Plans are available and accessible.
- 12.4. Ensure that the DR site has basic security (physical and environmental) in place.

13. CONDITION 13: CERTIFICATE ATTRIBUTES

The Licensee shall:

- 13.1. Ensure that the following certificate attributes are in place: certificate policy; usage parameters; expiration parameters; and distinction between the Licensee's certificate and the user's certificate.
- 13.2. Ensure that distinguished name fields and other information of users that may be used in social engineering are not part of certificate attributes:

14. CONDITION 14: CERTIFICATE REGISTRATION PROCESS

The Licensee shall implement authentication methods to verify the certificate applicant (Subscriber) and ensure retention of the authentication documents.

15. CONDITION 15: CERTIFICATE GENERATION PROCESS

The Licensee shall:

- 15.1. Adhere to the certificate generation process in accordance to the CP approved by the Authority.
- 15.2. Ensure that the information in the certificate is the same as in the request;
- 15.3. Ensure that the correct key pair is associated with the certificate information.

16. CONDITION 16: CERTIFICATE ISSUANCE PROCESS

The Licensee shall:

- 16.1. Ensure that the issuance channel used for the transmission of certificate, passwords and private keys between the Licensee and Subscribers is secure.
- 16.2. Put in place a mechanism to ensure that the receipt of certificates is acknowledged and accepted by the Subscribers.

17. CONDITION 17: CERTIFICATE PUBLICATION PROCESS

The Licensee shall:

- 17.1. Publish its certificate, CP, CPS and repository in a secure channel.

- 17.2. Ensure that the following information is available for the consumers to verify: Company Name; company Registration number; X500 name; internet address; telephone number; Licensee's certificate; and location of repository.
- 17.3. Obtain explicit consent for publication of Subscriber's certificate information.
- 17.4. Ensure that access to the repository is read-only to the public; subscribers and consumers; as restricted access to the Licensee's assigned personnel for updating the repository.
- 17.5. Ensure that modifications to the CPS are subject to a change management procedure of request and approval.

18. CONDITION 18: CERTIFICATE RENEWAL PROCESS

The Licensee shall ensure that certificate renewal requests are submitted using a secure channel or using the same authentication method in the registration process.

19. CONDITION 19: CERTIFICATE SUSPENSION PROCESS*

The Licensee shall:

- 19.1. Suspend the certificate when:
 - 19.1.1. Information marked with extension "critical" is suspected to be inaccurate;
 - 19.1.2. Private key or media holding the private key is suspected to be compromised;
 - 19.1.3. Subscriber is suspected to no longer be a member of the community subject to CP;
 - 19.1.4. The Subscriber requests it;
 - 19.1.5. Suspected violations of the generation or issuance process;
 - 19.1.6. Licensee's certificate is compromised.
- 19.2. Ensure that the suspended certificates are reactivated after investigations have been completed and no compromise has been confirmed.

- 19.3. Take steps to verify the identity of the requestor of the certificate suspension.
- 19.4. Ensure that information of suspended certificates are updated in the CRL and are digitally signed within one (1) hour upon verification that the suspension request is valid.
- 19.5. Take steps to ensure that the suspension information in the CRL is protected from unauthorized modifications.
- 19.6. Inform subscribers of the suspension within one (1) hour.

20. CONDITION 20: CERTIFICATE REVOCATION PROCESS

The Licensee shall:

- 20.1. Revoke the certificate when:
 - 20.1.1. Information marked with extension “critical” is inaccurate;
 - 20.1.2. Private key or media holding the private key is suspected or actually compromised;
 - 20.1.3. Subscriber is no longer a member of the community subject to CP;
 - 20.1.4. The Subscriber requests it;
 - 20.1.5. Suspected or actual violations of the generation or issuance process;
 - 20.1.6. Licensee’s certificate is compromised.
- 20.2. Take steps to verify the identity of the requestor of certificate revocation.
- 20.3. Ensure revocation information includes, but not limited to reason for revocation and revocation date/time.
- 20.4. Ensure that the certificate revocation information is digitally signed and published.
- 20.5. Inform the subscribers of the revoked certificates within one (1) hour.
- 20.6. Take steps to ensure that the certificate revocation information is protected from unauthorized modifications.

- 20.7. Ensure that revoked certificates are not re-activated.

21. CONDITION 21: CERTIFICATE ARCHIVAL PROCESS

The Licensee shall:

- 21.1. Ensure that all certificate suspension and revocation information, certificates, registration documents are archived for a minimum seven (7) years as required by the KICA 411A of 1998.
- 21.2. Test the archival process for accuracy, security and accessibility for digital archives.

22. CONDITION 22: AUDIT TRAILS

The Licensee shall:

- 22.1. Keep audit trails of certificate registration, generation, publication, issuance, renewal, suspension and revocation.
- 22.2. Keep system log files of security violations, errors, execution of privilege functions and changes in access control and system configurations.
- 22.3. Implement security mechanisms for the protection of audit trails.
- 22.4. Conduct reviews of the audit trails at least once every two (2) days trails and follow-up actions are performed within two (2) days.
- 22.5. Keep audit trails for at least twelve (12) months.

23. CONDITION 23: KEY GENERATION

The Licensee shall:

- 23.1. Ensure segregation of duties between personnel involved in system setup and maintenance and personnel involved in the key generation process.
- 23.2. Ensure that keys are stored under dual control.
- 23.3. Ensure separate key pairs exist for digital signature and encryption.

- 23.4. Ensure use of random key values in the generation of keys and that the seed (input) used in the random generator is not static and not predictable.
- 23.5. Review and approve the key generation system used by the Subscribers.

24. CONDITION 24: KEY DISTRIBUTION

The Licensee shall put in place procedures for transferring the keys from the key generation system to the storage device in a secure manner.

25. CONDITION 25: KEY STORAGE

The Licensee shall:

- 25.1. Provide Subscribers the necessary instructions and programs to safeguard and encrypt the Subscribers' private keys.
- 25.2. Store its keys in tamper proof devices.
- 25.3. Ensure that access to the tamper proof devices is dual controlled by personnel not involved in the setup, maintenance and operations of the Licensees systems; and documents and approves the change of Licensee's key custodians.
- 25.4. Ensure there are Licensee's key backup custodians to reduce key-man risks.

26. CONDITION 26: KEY USAGE

The Licensee shall:

- 26.1. Implement dual control loading of the certificates.
- 26.2. Perform integrity checks prior to loading of the certificates.

27. CONDITION 27: KEY BACKUPS

The Licensee shall:

- 27.1. Ensure that private keys are backed up.
- 27.2. Store its backup keys in a separate physical location as the original key.

28. CONDITION 28: KEY CHANGE

The Licensee shall:

- 28.1. Ensure change of the Licensee and Subscriber keys periodically.
- 28.2. Provide notice to the Subscribers' relying parties of new key pairs used to sign certificates; and the Subscriber or owner of a changed key in a secured manner.
- 28.3. Put in place a key interlock procedure and implement the procedure during key change.

29. CONDITION 29: KEY DESTRUCTION/TERMINATION

The Licensee shall archive and securely store the backup copies upon the termination of a its signature private key.

30. CONDITION 30: KEY COMPROMISE

The Licensee shall:

- 30.1. Put in place an escalation process in the event of suspected or actual key compromise.
- 30.2. Inform the Authority within 24 hours of suspected or actual key compromise.
- 30.3. Ensure that all affected Subscriber certificates are revoked in the event its private key is compromised.
- 30.4. Ensure revocation of all affected keys and certificates in the case of subscriber private key compromise.

31. CONDITION 31: KEY ARCHIVAL

The Licensee shall:

- 31.1. Archive all its Public keys (permanently) and all Subscriber encryption (private) keys.
- 31.2. Ensure that the archives are protected from unauthorized modification.

32. CONDITION 32: SYSTEM CONTROLS

The Licensee shall:

- 32.1. Ensure access control matrixes (physical and logical) are defined for all operating systems, network devices, applications and databases used in the its operations exist. The access control matrixes should include, but not limited to personnel names, access granted, validity of access rights and the next access control matrix review date.
- 32.2. Ensure the application and currency/validity of the access controls defined in the access control matrixes.
- 32.3. Perform an assessment of its infrastructure components, which includes operating system, network devices, security software (e.g. Intrusion Detection System and Antivirus Software).
- 32.4. Ensure that there is a full assessment for new components and an incremental assessment for updates or modifications to the infrastructure.
- 32.5. Perform scans using tools of its systems and network devices to identify security vulnerabilities at least once a week. The tools must be able to scan system and network vulnerabilities. Follow-up actions from the scans shall be performed within a week.
- 32.6. Deploy an Intrusion Detection System (IDS) that covers 100 percent of components of its infrastructure. Follow-up actions on potential intrusions shall be performed within a week.
- 32.7. Perform regular log review (using the access control matrixes) of unauthorized access and modifications to key system files and utilities; and unauthorized access and modifications of Subscribers' data. Follow-up actions on identified unauthorized access shall be performed within a week.

33. CONDITION 33: PHYSICAL SECURITY

The Licensee shall ensure that:

- 33.1. The location of its systems is not publicly identified;

- 33.2. Physical security systems are installed;
- 33.3. Inventory of access control cards are at least dual-controlled;
- 33.4. Loss of access control cards are reported and follow-up actions are performed;
- 33.5. Systems performing certification should be partitioned under lock and key;
- 33.6. Entry to the partition must be logged with timestamps;
- 33.7. Entry logs are reviewed regularly;
- 33.8. Access to infrastructure components (power control, communication riders and cabling) is restricted to authorized personnel;
- 33.9. An approval process for temporal or bypass access exists;
- 33.10. An Intrusion Detection System (IDS) exists.

34. CONDITION 34: GENERAL SECURITY CONTROLS

The Licensee shall ensure that:

- 34.1. Systems performing certification functions are not used for general purposes (e.g. word processing, emailing, web surfing);
- 34.2. Strong password policies are implemented;
- 34.3. Inactive lockouts are implemented (no longer than 10 minutes of inactivity before lockout);
- 34.4. Updated security patches are reviewed, tested, applied and implemented.

35. CONDITION 35: CHANGE AND CONFIGURATION MANAGEMENT

The Licensee shall ensure that:

- 35.1. All changes are supported by change requests;
- 35.2. All change requests are approved before construction;

- 35.3. All source codes should be version-controlled;
- 35.4. There is an approved process of moving from development to production;
- 35.5. Segregation of duties exists for source code migration.
- 35.6.

36. CONDITION 36: NETWORK SECURITY

The Licensee shall ensure that:

- 36.1. Network access control exists to separate and isolate its systems from the other systems;
- 36.2. Communications between its systems are secured and data is not transmitted in clear text format;
- 36.3. An IDS is present and that the IDS monitors its systems.

37. CONDITION 37: APPLICATION INTEGRATION CONTROLS

The Licensee shall ensure that the application toolkits it provides to the user and developer community complies with the following:

- 37.1. The user is informed when a private key is being accessed;
- 37.2. The user is alerted if its private key is being used for a purpose that is not consistent with that defined as acceptable use by the issuer;
- 37.3. Mechanisms are available to check the integrity of the applications for unauthorized modifications, especially the integrity of signing and verification functions;
- 37.4. Application security risk assessment on the Licensee's software infrastructure is conducted yearly to ensure that the software that manages, issues and revokes certificates is developed to manage the risk identified;
- 37.5. The application securely purges the private key temporarily stored for processing to minimize private key exposure;
- 37.6. The application verifies the validity and authenticity of the certificate;

- 37.7. The verification process traces and verifies all the components in the certification path;
- 37.8. For validity and authenticity verification, is necessary to verify that the certificate issuer's signature is valid; the certificate is valid (i.e. has not expired, been suspended or revoked); and the certificate extensions flagged as "critical" are being complied with.

38. CONDITION 38: PROVISION OF CONSUMER INFORMATION SERVICES

- 38.1. Within NINE (9) months from the Effective Date, the Licensee shall establish and maintain efficient information services to assist any person to answer questions regarding products, services, and any other reasonable questions relating to the Licensed Services.
- 38.2. The obligation in 38.1 shall not apply in the event that it is not, in the Authority's view, reasonable to require the Licensee to provide the service requested.

39. CONDITION 39: REQUIREMENT TO PUBLISH THE CHARGES, TERMS AND CONDITIONS OF LICENSED SERVICE

- 39.1. At least one month prior to offering a Licensed Service or adjusting the charges, terms and conditions of an existing service, the Licensee shall file the following for approval, with the Authority:
- 39.1.1. the description and scope of the service,
 - 39.1.2. terms and conditions of the service,
 - 39.1.3. dispute resolution mechanisms, and
 - 39.1.4. charges, (excluding special offers) upon which it proposes to offer the Licensed Services
- 39.2. The Licensee shall provide the Licensed Services on Charges, Terms and Conditions approved in accordance with 39.1. A copy of the current version of the Charges, Terms and Conditions shall be published and provided to any person who reasonably requests.
- 39.3. Notwithstanding condition 39.1 and 39.2, the Licensee shall ensure that the charge for each service is clearly stated in all promotions.

- 39.3.1. Prices must be noted in the form of a numerical price, inclusive of all taxes, or the total cost to the Consumer of a service:
- 39.3.2. Textual pricing information must be legible, prominent, horizontal and presented in a way that does not require close examination.
- 39.3.3. In the case of promotions transmitted via audio-visual device such as television broadcast, the pricing information must be spoken as well as visually displayed.
- 39.4. In any case, the Licensee shall place a short, distinct pricing message during a service promotion.
- 39.5. No product or service may be promoted as being free or being described in a way that implies it is free if it attracts a charge.

40. CONDITION 40: INTERCONNECTION & PROTECTION OF THIRD PARTY FACILITIES

- 40.1. The Licensee shall enter in to Service Level Agreements (SLA) with other licensees for the provision of the Licensed Services.
- 40.2. The Licensee shall install suitable equipment for compatibility with the systems of other licensees so as to enable the provision of the Licensed Services.
- 40.3. The Licensee shall ensure that its equipment, facilities, or operations do not interfere, damage or harm any third party property, systems, installations, facilities, or operations.
- 40.4. In case such damage, harm or interference should occur, the Licensee shall immediately switch off its offending equipment, facilities or operations and inform the Authority and the affected operator as a matter of urgency.
- 40.5. Such information shall in no way prejudice the Authority's or third party rights or claims they may have against the Licensee for the interference, damage, harm or for financial loss that may have been occasioned.
- 40.6. The Licensee shall render the said equipment, facilities or operations harmless and/or compensate those third parties that may suffer damage, as a result of its equipment, facilities, systems or operations causing harm or interference.

41. CONDITION 41: INTERRUPTIONS TO THE LICENSED SERVICES

- 41.1. The Licensee shall not intentionally interrupt, suspend nor terminate the provision of any type of Licensed Service without having first notified the Authority in writing and having provided reasonable advance notice to persons affected by such interruption, suspension or termination.
- 41.2. In the event of an unintentional/unforeseen interruption of the Licensed Services or part thereof, which are significant in nature, the Licensee shall inform the public and notify the Authority in writing within 24 hours outlining the cause of such interruption and the steps being undertaken to rectify such interruption.
- 41.3. The provision in 41.1 shall not apply if, the interruption or suspension is to a person to whom the Licensee provides the Licensed Service and whose system or apparatus (or use thereof) is endangering the integrity of the Licensee's operations.
- 41.4. The provision in 41.1 shall not apply if the interruption of service is the result of Consumer's non-payment or other business related or contractual reasons.

42. CONDITION 42: AUDIT AND INSPECTION

The Licensee shall permit the Authority (or an independent auditor appointed by the Authority) to audit and/or inspect its premises, facilities, files, records and other data to enable it to exercise its functions under the Act.

43. CONDITION 43: BILLING ACCURACY

- 43.1. The Licensee shall, prior to the commencement of Licensed Systems, establish a procedure to ensure the accuracy of its billing system, which must be submitted to the Authority for approval. Such an approval shall not be unreasonably delayed or withheld and in any event, the Authority shall give its approval or disapproval within three (3) months from date of receipt of the said submission.
- 43.2. The Authority shall reserve the right to examine the billing system before and after it is operational in order for the Authority to be satisfied that the billing process has the characteristics required as set out above. The Authority (or

an independent auditor appointed by the Authority) may require the Licensee to:

- 43.2.1. furnish the Authority with any information it reasonably requires;
- 43.2.2. on reasonable notice, allow the Authority (or any person authorised by the Authority) access to any relevant premises of the Licensee, and
- 43.2.3. on reasonable notice, allow the Authority (or any person authorised by the Authority) to examine or test the whole or any part of the billing process.
- 43.3. Where the Authority gives the terms of its approval or disapproval, pursuant to Condition 43.1 and 43.2, it is agreed that the Licensee shall take all reasonable steps to comply with such terms issued by the Authority within the shortest time possible but in any event not more than thirty (30) days from the date the terms are issued.
- 43.4. The Licensee shall not render any bill in respect of any Licensed Systems unless every amount stated in the bill is derived in accordance with the procedure agreed with the Authority in 43.1 or/and 43.2 above.
- 43.5. The Licensee shall keep such records as may be necessary or may be determined by the Authority to be necessary for the purpose of satisfying the Authority that the billing process has the characteristics required above and shall retain any records for more than two (2) years from the date on which they came into being.
- 43.6. Any changes to the Licensee's billing system shall be notified to the Authority and shall be subject to the requirements under this Condition.

44. CONDITION 44: PRIVACY AND CONFIDENTIALITY

- 44.1. The Licensee shall use all reasonable endeavours to ensure the privacy and confidentiality of proprietary information and business secrets obtained in the course of its business from any person to whom it provides the Licensed services by establishing and implementing reasonable procedures for maintaining confidentiality of such information.
- 44.2. The Licensee shall maintain sufficient information on its confidentiality procedures to satisfy the Authority, at its reasonable request, that the requirements of 44.1 are being met.

- 44.3. The Licensee shall obtain explicit permissions from the Subscribers for third party disclosure as necessary for the provision of the Licensed service.
- 44.4. The Licensee shall not use or allow to be used any apparatus comprised in the Licensed Services (except for the purpose of law enforcement, national interest or where it is in accordance with any statute in force in Kenya) which is capable of recording, silently monitoring, or intruding into its Subscriber's communications traffic unless the Licensee complies with 44.4 and 44.5 below.
- 44.5. Except for the purposes of law enforcement, the Licensee shall make every reasonable effort to inform the parties whose traffic is to be recorded, silently monitored or intruded into before commencing the recording, silent monitoring or intrusion, that the traffic is to be or may be recorded, silently monitored or intruded into.
- 44.6. The Licensee shall maintain a record of the means by which the parties have been informed that their traffic is to be or may be recorded, silently monitored or intruded into and the purpose of such recording. The Licensee shall furnish the Authority with such information on request.

45. CONDITION 45: FAIR TRADING

- 45.1. Without prejudice to other obligations imposed on the Licensee under this Licence, the Licensee shall not engage in any activities, whether by act or omission, which have, or are intended to or likely to have, the effect of unfairly preventing, restricting or distorting competition in Kenya (or a part of it), in relation to any business activity relating to the Licensed Services. Without limiting the generality of the foregoing, any such act or omission shall include:
- 45.1.1. any abuse by the Licensee, either independently or with others, of a dominant position in Kenya which unfairly excludes or limits competition between the Licensee and any other party;
- 45.1.2. entering into any contract or engaging in any concerted practice with any other party, which unfairly prevents, restricts or distorts competition in Kenya, or

- 45.1.3. effecting anti-competitive changes in the communications market in Kenya, and in particular, anti-competitive mergers and acquisitions in the communications sector.
- 45.2. In the event it appears to the Authority that the Licensee is in breach of 45.1, the Authority shall give written notice to the Licensee:
- 45.2.1. stating that the Authority is investigating a possible contravention;
- 45.2.2. setting out detailed reasons why it appears to the Authority that there is a breach by the Licensee of this Condition, and
- 45.2.3. setting out the steps the Authority believes the Licensee should take in order to remedy the alleged breach and giving the Licensee a reasonable time in which to correct the alleged breach.
- 45.3. The Authority shall allow the Licensee thirty (30) days from the date of the notice to make representations to the Authority, before the Authority takes further action.

46. CONDITION 46: PROHIBITION ON UNDUE DISCRIMINATION

- 46.1. Subject to 46.3 without prejudice to the obligations imposed on the Licensee under this Licence, the Licensee shall not (whether in respect of the rates or other terms and conditions applied or otherwise) show undue preference to, or exercise undue discrimination against, particular persons or persons of any class or description in respect to the provision of the Licensed Services.
- 46.2. Subject to 46.3 the Licensee may be deemed to have shown such undue discrimination if it unfairly favours to a material extent the provision of any communications services to another communication business it carries out so as to place at a significant competitive disadvantage persons competing with that business.
- 46.3. The Licensee shall not be deemed to have shown undue discrimination to the extent that:
- 46.3.1. it is due to matters beyond the Licensee's control;
- 46.3.2. the provision of electronic certification services would expose any person engaged in its provision to undue risk of health or safety, or

46.3.3. it is not, in the Authority's view, reasonably practicable or technically feasible to provide electronic certification services to the person.

46.4. Any question relating to whether any act done or course of conduct amounts to undue preference or undue discrimination shall be determined by the Authority.

47. CONDITION 47: PROHIBITION OF CROSS-SUBSIDIZATION

47.1. The Licensee shall not subsidise or cross-subsidise, or permit itself to be subsidised or cross-subsidised or give or receive undue preference to or from, as the case may be, any of its associated businesses or persons as concerns the provision of the Licensed Services and/or any other licences granted to the Licensee by the Authority.

47.2. The Licensee shall maintain necessary records to evidence resource transfers between its associated businesses or persons. The Authority may at its discretion request the licensee to submit this or other information related to the licensed businesses to satisfy the Authority that no cross-subsidy is taking place.

47.3. In the event that the Authority determines that cross-subsidy has occurred the Authority shall give written notice to the licensee setting out the steps the Authority believes the Licensee should take in order to remedy the alleged breach and giving the Licensee a reasonable time in which to correct the alleged breach. The Authority shall allow the Licensee thirty (30) days from the date of the notice to make representations to the Authority, before the Authority takes further action.

47.4. Where the Authority deems it necessary and appropriate to supervise compliance with the provisions of this Licence, it may order the Licensee to provide the Licensed Services through a separate division or divisions, a separate branch or branches or a separate subsidiary or subsidiaries.

48. CONDITION 48: NOTIFICATION OF CHANGE IN SHAREHOLDING

48.1. Subject to 48.3 below, the Licensee shall notify the Authority of:

48.1.1. any change in the proportion of the shares held directly in a Licensee by any person, and

- 48.1.2. the acquisition of any shares and such shares not being shares already listed in any stock exchange held directly in a Licensee by a person not already holding shares, and the proportion of such shares held by that person immediately before acquisition.
- 48.2. The Licensee shall notify the Authority prior to any entity acquiring ownership or control of all or a majority of the stock of the Licensee such that the Licensee shall stand as a subsidiary in relation to that entity.
- 48.3. The Licensee shall be obliged to notify the Authority of any acquisition of shares or change in shareholding of the Licensee by any person and such shares not being shares already listed in any stock exchange only if, by reason of that acquisition or change, the total number of shares in the Licensee held by that person together with any shares held by any nominee or trustee for that person immediately after the change or acquisition:
- 48.3.1. exceeds 15 per cent of the total number of shares in the Licensee (where it does not exceed 15 per cent prior to that change or acquisition);
 - 48.3.2. exceeds 30 per cent of the total number of shares in the Licensee (where it does not exceed 30 per cent prior to that change or acquisition), and
 - 48.3.3. exceeds 50 per cent of the total number of shares in the Licensee (where it does not exceed 50 per cent prior to that change or acquisition).
- 48.4. In any case referred to in 48.1 or 48.2, notification shall be given by a date, which is thirty (30) days prior to the taking effect of such change or acquisition, as the case may be.
- 48.5. In instances referred to in 48.2 and 48.3, if the Authority disapproves of the change in shareholding notified to it, it shall notify the Licensee within thirty (30) days of receipt of notification. The Authority may within sixty (60) days of notifying the Licensee of its disapproval, having taken into account representations made by interested parties, and giving reasons for its decision, prohibit the change in shareholding where it believes it is in the public interest to do so.

49. CONDITION 49: PRE-NOTIFICATION OF JOINT VENTURES

- 49.1. The Licensee shall notify the Authority not later than thirty (30) days before the taking effect of any of the agreements or arrangements to which this Condition applies giving particulars of the agreements and/or arrangements.

The agreements or arrangements are an agreement with any person for the establishment or control of anybody corporate for the purpose of:

- 49.1.1. the running of a communications system which requires a licence under the Act;
 - 49.1.2. providing communications services in Kenya which requires a licence under the Act;
 - 49.1.3. carrying of content over communications systems which requires a licence under the Act;
 - 49.1.4. the production of communications apparatus for supply in Kenya where that production would lead, in the Authority's view, to a monopoly situation which would not otherwise exist in relation to the supply of communications apparatus of any description in Kenya;
 - 49.1.5. an agreement for the establishment of a partnership for any of those purposes and in those circumstances, and
 - 49.1.6. any other agreement or arrangement in the nature of the joint venture for the purpose of running a business which requires a licence under the Act or for the purpose of providing communications services in Kenya.
- 49.2. above applies in relation to an agreement or arrangement for the establishment or control of any body corporate or partnership where the Licensee has or is to have not less than twenty (20) per cent of the voting power in any organ controlling that body.

50. CONDITION 50: ACCOUNTING REQUIREMENTS

- 50.1. Within nine (9) months from the Effective Date, the Licensee shall submit to the Authority the accounting principles which relates to the running of the Licensed Services and which allows the recording of investments, expenses and revenues in accordance with accounting standards recognised in Kenya.
- 50.2. Within ninety (90) days of the end of each fiscal year of the Licensee, the Licensee shall deliver to the Authority its balance sheet as at the end of such fiscal year and the related statements of operations, equity and cash flows, in each case accompanied by a report thereon of independent auditors stating that such financial statements fairly present the financial position of the Licensee at the dates indicated and were prepared in accordance with

accounting principles submitted to the Authority in accordance with 50.1 above.

- 50.3. The Authority may request the Licensee to submit other accounting information it may require in order to effectively supervise and enforce the terms of this Licence and in particular if the accounting principles established by the Licensee fail to achieve the objectives set forth in that Condition.

51. CONDITION 51: REQUIREMENT TO PROVIDE INFORMATION

- 51.1. The Licensee is required to maintain such information as will enable the Authority to carry out its functions under the Act in such manner and at such times as the Authority may request.
- 51.2. The Authority shall have the right to request the Licensee to submit periodic reports, statistics and other data as well as request additional information with a view to supervise and enforce effectively the terms of this Licence.
- 51.3. In particular, by the 15th July of every year or as agreed by the Authority, the Licensee shall submit a Compliance Report detailing the performance of the previous operational year ended 30th June.
- 51.4. The Authority shall review the Compliance Report and:
- 51.4.1. If the Licensee is in compliance with the Licence, issue the Licensee with a Compliance Certificate in respect of compliance for the year under review, and
 - 51.4.2. If the Licensee is not in compliance with the Licence, require the Licensee to remedy the area of non-compliance in accordance with the provisions of this Licence and the Act.
- 51.5. In making a request for information, the Authority will ensure that no undue burden is imposed on the Licensee in procuring and furnishing such information, unless the Authority considers such information is essential to enable it to exercise its functions under the Act.
- 51.6. The Authority shall have the right to publish information which it receives under this Condition unless, following representations by the Licensee, the Authority is satisfied that the information is of such confidential nature that disclosure would have a material adverse effect on the Licensee's business.

52. CONDITION 52: DISPUTE SETTLEMENT

The dispute settlement mechanism set out in the Act and Regulations shall apply to any dispute or disputes that arise out of the provisions of this Licence.

53. CONDITION 53: LICENCE REVOCATION

Notwithstanding any other Condition in this License, the Authority may at any time revoke this Licence by giving six (6) months' notice in writing in any of the following circumstances:

- 53.1. if the licensee communicates to the Authority in writing on their intention to terminate the Licence;
- 53.2. if the Licensee does not provide evidence of commencement of the provision of the Licensed Services fifteen (15) months from the Effective Date. The Licensee shall submit such evidence by completing a Compliance Report in order to satisfy the Authority that the Licensee has complied with this requirement;
- 53.3. if any amount payable under Conditions 56 is unpaid forty-five (45) days after the Authority notifies the Licensee that the payment is overdue, such notification not to be given earlier than fourteen (14) days after the date on which the payment is due;
- 53.4. if the Licensee has breached a Condition in this Licence, and in the Authority's opinion the breach is of a material nature, and the Licensee has failed to comply with any notice issued by the Authority under the Act or under the Regulations and thereafter has been given by the Authority a further sixty (60) days in which to make representations in relation to the matters set out in the earlier notice which the Authority has taken into account or matters which the Licensee believes are relevant and the Authority appears not to have taken into account;
- 53.5. if the Licensee is dissolved or enters into liquidation, bankruptcy or equivalent proceedings or makes a general assignment for the benefit of creditors, and
- 53.6. if the Licensee fails to notify the Authority of any of the events specified in Condition 48 or 49 and the Authority has given written notice to the Licensee that the Authority intends to revoke the Licence on the grounds set out in Condition 48 or 49 respectively.

After the end of the six (6) months' notice, the Authority shall publish a notice in the Kenya Gazette stating that it intends to revoke this Licence and setting out the reasons on which this intention is based. Revocation shall take effect seven (7) days following publication of the notice in the Kenya Gazette.

54. CONDITION 54: LICENCE RENEWAL

The Authority may renew this Licence at the request of the Licensee following the expiry of the Licence Period for an additional ten (10) years provided that the Authority has carried out a formal review to determine whether or not the Licence should be renewed, which review shall be concluded two (2) years prior to the expiry of the Licence Period.

55. CONDITION 55: LICENCE TRANSFER

The Licensee shall not assign, delegate, transfer or encumber in any manner the rights, interests or obligations under this Licence without the prior, express and written consent of the Authority, such consent not to be unreasonably withheld or delayed.

56. CONDITION 56: LICENCE FEES

The Licensee shall pay to the Authority:

- 56.1. An initial Licence fee amounting to Kenya Shillings one hundred thousand (KShs.100,000) and an upfront operating fee amounting to Kenya Shillings Eighty thousand (KShs.80,000).
- 56.2. On 1st July of each year, an annual operating fee equivalent to zero-point-four percent (0.4%) of the audited annual gross revenues accruing from the Licensed Services during the previous financial year or Kenya shillings Eighty thousand (KShs. 80,000) only whichever is higher.
- 56.3. Any other fee payable under this Licence.

Signed for and on behalf of the Authority

Director General

Date



ANNEX 1: ROLL OUT REQUIREMENTS

Describe the nature of roll out.....

Period	Areas
Year 1	Nairobi City
Year 2	Nairobi City, Mombasa City, Kisumu City
Year 3	At least 25% of Counties
Year 4	At least 50% of Counties
Year 5	At least in every County

ANNEX 2: APPLICABLE PENALTIES

The Licensee shall be subject to penalties as described in Section 26 of the Act. Unless otherwise stated, failure to comply with any of the Licence Conditions above will constitute a contravention which may be subject to a penalty.

In the event that the Licensee fails to remedy any contravention within three months after notification by the Authority, the Licensee shall be subject to a penalty of Kenya shillings five hundred thousand (Kshs 500,000) only for each contravention for every month or part thereof during which the contravention continues.

