GOVERNMENT OF ZAMBIA

Statutory Instrument No. 71 of 2011

The Electronic Communications and Transactions Act, 2009

The Electronic Communications and Transactions (General) Regulations, 2011

ARRANGEMENT OF REGULATIONS

PART I

PRELIMINARY

Regulations

1. Title
2. Application
3. Interpretation

PART II

REGISTRATION OF CRYPTOGRAPHY SERVICE PROVIDERS

4. Application for registration as cryptography service provider
5. Registration as cryptographer service provider
6. Changes in detail or nature of cryptography services
7. Surrender of certificate of registration
8. Prohibition on assigning, ceding or transferring certificate of registration
9. Application for consent to assign, cede etc, certificate of registration
10. Renewal of certificate of registration
11. Suspension or revocation of certificate of registration
12. Register of cryptography service providers

Copies of this Statutory Instrument can be obtained from the Government Printers, P.O. Box 30136, 10101 Lusaka Price K38,000 each.
PART III

ACCREDITATION OF AUTHENTICATION SERVICE PROVIDERS

13. Provision of authentication products or services
14. Application for accreditation of authentication product or service
15. Accreditation as authentication product or service provider
16. Changes in detail or nature of authentication products or services
17. Surrender of accreditation
18. Prohibition of assigning, ceding or transferring accreditation without authority
19. Application for approval to assign, cede or transfer accreditation
20. Renewal of accreditation
21. Suspension or revocation of accreditation
22. Database of authentication service providers
23. Minimum compliance requirements for authentication

PART IV

TECHNICAL REQUIREMENTS FOR AUTHENTICATION AND CERTIFICATION

24. Issuance of authentication certificates
25. Requirements for certification practice statements
26. Duties of subscribers
27. Responsibilities of certification service providers
28. Record keeping
29. Suspension and revocation of certificates
30. Adherence to international standards, risk assessments and audits
31. Recognition of foreign accreditation
PART V
PROTECTION OF CRITICAL DATABASES
32. Declaration of critical databases
33. Registration and identification of critical databases
34. Management of critical databases
35. Access to, transfer and control of critical databases
36. Securing integrity and authenticity of critical data
37. Procedures and technological methods for use in storage or archival of critical databases
38. Disaster recovery plans
39. Risk assessment and evaluation of critical databases

PART VI
INTERCEPTION OF ELECTRONIC COMMUNICATIONS
40. Interception capability of electronic communications services
41. Duration of interception capability
42. Non-detectability of interception
43. Technical arrangements for interception
44. Configuration of interception capable networks, services or archives
45. Restrictions on implementation of interception measure
46. Routing, provisioning storage, etc. of real-time and archived communications
47. Availability, storage, archival, etc. of real time communication related information
48. Information safety, security, etc.
49. Technical standards and configuration for real time and archived communication-related information
50. Storage period for communications
PART VII
DETAILLED SECURITY, FUNCTIONAL AND TECHNICAL REQUIREMENTS FOR INTERCEPTION

51. General security, functional and technical requirements
52. Detailed security, functional and technical requirements for public switched telecommunications networks, fixed networks and mobile communications networks
53. Detailed security, functional and technical requirements for internet service providers
54. Technical security standards for public switched telecommunications networks, fixed networks and mobile communications networks
55. Technical security standards for internet service providers

PART VIII
GENERAL PROVISIONS

56. Fees
57. Transitional provision
FIRST SCHEDULE
SECOND SCHEDULE
In exercise of the powers contained in sections thirty-three, forty-four, seventy-nine and one hundred and thirteen of the Electronic Communications and Transactions Act, 2009, the following Regulations are hereby made:

PART I

PRELIMINARY

1. These Regulations may be cited as the Electronic Communications and Transactions (General) Regulations, 2011.

2. These Regulations shall apply to the importation, supply, interception, accreditation, protection, utilisation, encryption and identification of electronic communications apparatus and services.

3. In these Regulations, unless the context otherwise requires
   “archive” means the storage of data in a format where the data is not actively used but can be accessed at any time when required, and includes the storage of data by third parties, and “archived” or “archival” shall be construed accordingly;
   “authentication certificate” means a certificate issued by a certification Authority or trusted third party that verifies the authentication of a certificate related to encryption that is issued by an authentication product or service provider;
   “authorised officer” means any person authorised by the Authority to act on its behalf;
   “Authority” has the meaning assigned to it in the Act;
   “buffer” means the temporary storage of communication-related information in case the necessary electronic communication connection to route information to the Monitoring Centre is temporarily unavailable, and “buffered” shall be construed accordingly;
   “certificate of accreditation” means a certificate issued to a person upon registration as an accreditation service provider;
   “certificate of registration” means a certificate issued to a person upon registration as a cryptograph service provider;
   “certification Authority” means an authority of a network that issues and manages security credentials and public keys for message encryption;

Title

Application

Interpretation

Act No. 15 of 2009
“connection” means a physical or logical linking between two or more electronic communications apparatus used by the same or different electronic communications service providers resulting in the transfer of an information unit or data capable of allowing one user of an electronic communications service to communicate with another user or to access a service provided by a third party;

“electronic communications apparatus” has the meaning assigned to it in the Information and Communication Technologies Act, 2009;

“fixed line” means an electronic communications network or service which uses fixed line technology deployed in its electronic communications system;

“handover interface” means a physical and logical interface across which the results of an interception of communication order or request are delivered from the electronic communications network or service provider to the Monitoring Centre;

“identity” means a technical label which represents the origin or destination of an electronic communications traffic, as a rule clearly identified by a logical or virtual electronic communications identity number assigned to a physical access;

“interception of communications order” means an order made by a court pursuant to section sixty-six of the Act;

“interception measure” means a technical measure that facilitates the interception of electronic communications traffic or data pursuant to the Act;

“interception target” means a person whose indirect communications are to be intercepted, or whose real time communication-related information or archived communication-related information is to be routed by an electronic communications network or service provider to the Monitoring Centre or provided to a law enforcement agency, pursuant to an interception of communications order or request;

“International Mobile Equipment Identity (IMEI)” means a number that uniquely identifies cellular mobile equipment;

“internet service” means connectivity or access to a public transmission control protocol/internet protocol (TCP/IP)
network or services layered over transmission control protocol internet protocol (TCP/IP) such as web, email, file transfer, web mail, online chat and voice over IP (VoIP) telephony;

“internet service provider” means an electronic communications service provider providing internet services;

“IPSec” means Internet Protocol Secure, an industry standard, security protocol utilising modern data cryptographic techniques for the establishment of a secure tunnel;

“licensee” has the meaning assigned to it in the Information and Communication Technologies Act;

“link” means a physical or logical connection between two points;

“mobile cellular service provider” means an electronic communication service provider licenced to provide mobile telecommunications under the Information and Communication Technologies Act, 2009;

“Mobile Subscriber Integrated Service Digital Network (MSISDN)” means a number uniquely identifying a subscription in a Global System for Mobile (GSM) or Universal Mobile Telecommunication System (UMTS) mobile network;

“Monitoring Centre” has the meaning assigned to it in the Information and Communication Technologies Act, 2009;

“quality of service” in relation to an interception measure means the capability of a network to provide service to network traffic over various technologies to a standard which ensures that different priority is provided to different applications, user or data flows to guarantee a determined acceptable level of end-to-end performance without the deterioration of the end-to-end performance as a result of the interception measure;

“result of interception” means the content of an indirect communication which is routed by an electronic communications network or service provider to the Monitoring Centre pursuant to an interception of communication order or a request;

“request” means a request made in terms of sections sixty.
seven and sixtyeight of the Act;

“secure tunnel” means an encrypted and authenticated internet protocol (IP) communication channel established using the most recently published versions of the IPSec Transport Layer Security (TLS), or Secure Socket Layer (SSL) protocols;

“seller” means a person or an agent appointed by the mobile cellular service provider or authorised to sell SIM cards on the mobile cellular service provider’s behalf;

“SIM card” means a Subscriber Identification Module (SIM) card inserted inside the mobile cellular phone or other device;

“successful call” means the successful establishment of a communication channel with the generation of one or more call data records (CDRs) associated with the communication channel;

“target identity” means the identity associated with a target service, used by the interception target; and

“target service” means an electronic communications service associated with an interception target and usually specified in an interception of communications order or request.

PART II
REGISTRATION OF CRYPTOGRAPHY SERVICE PROVIDERS

4. (1) A person who wishes to provide a cryptography service shall apply to the Authority in Form I set out in the First Schedule.

(2) The Authority shall, within seven days of receipt of an application under sub-regulation (1), approve or reject the application.

5. The Authority shall, where—

(a) the application meets the requirements of these Regulations, approve the application and issue a certificate of registration in Form II set out in the First Schedule; or

(b) the application does not meet the requirements of these Regulations, reject the application and inform the applicant of the rejection in Form III set out in the First Schedule.
6. (1) A cryptography service provider shall notify the Authority of any change in the particulars relating to the registration of that cryptography service provider in Form IV set out in the First Schedule.

(2) A cryptography service provider shall, where the cryptography service provider intends to change the nature of the cryptography services provided, apply to the Authority for a variation or amendment of the nature of the service in Form V set out in the First Schedule.

(3) The Authority shall—

(a) where it approves an application made under sub-regulation (1) inform the applicant of the approval and endorse the change in particulars or variation of the nature of the cryptography service provided, as the case may be, on the certificate of rejection; or

(b) where it rejects an application, inform the applicant of the rejection in Form III set out in the First Schedule and endorse the rejection on the certificate of rejection.

7. (1) Where a cryptography service provider does not intend to continue with the services to which the certificate of registration relates, the cryptography service provider shall notify the Authority in Form VI set out in the First Schedule and shall agree with the Authority on the terms and conditions of the surrender of the certificate of registration with particular reference to anything done or any benefit obtained under the certificate of registration.

(2) Where a certificate of registration is surrendered under sub-regulation (1)—

(a) the certificate of registration shall lapse or be cancelled and the cryptography service provider shall cease to be entitled to any benefits obtainable under the certificate of registration; and

(b) the Authority shall inform the cryptography service provider of the lapse or cancellation in Form VII.

8. A cryptography service provider shall not assign, cede or otherwise transfer a certificate of registration to any other person without the prior approval of the Authority.

9. (1) An application for consent to assign, cede or otherwise transfer a certificate of registration shall be in Form VIII set out in the First Schedule.
(2) The Authority shall—

(a) where it approves an application made under sub-regulation (1), inform the applicant of the approval in Form IX set out in the First Schedule and endorse the approval on the certificate; or

(b) where it rejects an application under sub-regulation (1), inform the applicant of the rejection in Form III set out in the First Schedule.

10. (1) An application for the renewal of a certificate of Registration, in Form X set out in the First Schedule.

(2) The Authority shall, where an applicant complies with the provisions of these Regulations or the conditions of a certificate of registration, renew the certificate of registration and endorse the renewal on the certificate.

(3) The Authority shall where it rejects an application made under sub-regulation (1), inform the applicant of the rejection in Form III set out in the First Schedule.

11. (1) The Authority may suspend or revoke a certificate of registration, after investigation and upon according the cryptography service provider an opportunity to be heard, if the cryptography service provider—

(a) obtained the certificate of registration by fraud, misrepresentation or any false or misleading statement;

(b) assigns, cedes or otherwise transfers the certificate of registration to another person without the prior approval of the Authority;

(c) fails without reasonable explanation to provide the services described in the certificate of registration;

(d) breaches or otherwise fails to comply with any terms or conditions of the certificate of registration; or

(e) is convicted of an offence under the Act or any other written law for which the punishment is a term of imprisonment for a period exceeding six months.

(2) The Authority shall, before taking any action under sub-regulation (1), notify the cryptography service provider of its intention to suspend or revoke the certificate of registration in Form XI set out in the First Schedule.

(3) The Authority shall not suspend or revoke a certificate of registration where the holder takes remedial measures to the
satisfaction of the Authority, within such period as the Authority may specify.

(4) The Authority shall, where the Authority suspends or revokes a certificate, inform the holder of the suspension or revocation in Form XII set out in the First Schedule.

(5) Where a certificate of registration is suspended or revoked, its holder shall cease to be entitled to the rights or benefits conferred by or under these Regulations with effect from the date of the suspension or revocation and

(a) in the case of a suspension, for the period of the suspension; and

(b) in the case of a revocation, shall surrender the certificate of registration to the Authority immediately.

12. The Authority shall cause to be maintained a register of cryptography service providers which shall contain —

(a) the names and details of holders of certificates of registration under this Part;

(b) a description of the type of cryptography service or cryptography product provided;

(c) the conditions attached to each certificate of registration;

(d) the amendments, suspensions or revocations of certificates of registration; and

(e) such other particulars as may be necessary to identify and locate the cryptography service provider or the products or services adequately.

PART III
ACREDITATION OF AUTHENTICATION SERVICE PROVIDERS

13. (1) A person accredited under regulation 15 may provide an authentication product or service.

14. (1) A person who wishes to provide an authentication product or service shall apply to the Accreditation Authority in Form I set out in the First Schedule.

(2) The Authority shall, within seven days of the receipt of an application under sub-regulation (1), approve or reject the application.

(3) Where the Authority rejects an application for accreditation, it shall within seven days of its decision, inform the applicant of the rejection in Form III set out in the First Schedule.
15. The Authority shall —

(a) where an application meets the requirements of these Regulations, grant the accreditation in Form II set out in the First Schedule; or

(b) where an application does not meet the requirements of these Regulations, reject the application and inform the applicant of the rejection in Form III set out in the First Schedule.

16. (1) An authentication service provider shall notify the Accreditation Authority of any change in the particulars relating to the accreditation of the authentication service provider in Form IV set out in the First Schedule.

(2) An authentication service provider shall, where the authentication service provider intends to change the nature of the authentication products or services, apply to the Authority for a variation of the nature of the product or service in Form V set out in the First Schedule.

(3) The Authority shall—

(a) where it approves an application under sub-regulation (1), inform the applicant of the approval and endorse the change in particulars or variation of the nature of the cryptography service provided, as the case may be, on the accreditation; or

(b) where it rejects an application, inform the applicant of the rejection in Form III set out in the First Schedule and endorse the rejection on the accreditation.

17. (1) Where an authentication service provider ceases to provide the services to which the accreditation relates, the authentication service provider shall notify the Authority in Form VI set out in the First Schedule and shall agree with the Authority on the terms and conditions of the surrender of the accreditation with particular reference to anything done or any benefit obtained under the accreditation.

(2) Where an accreditation is surrendered under sub-regulation (1)—

(a) it shall lapse or be cancelled and the authentication service provider shall cease to be entitled to any benefits obtainable under the accreditation; and

(b) the Authority shall inform the authentication service provider of the lapse or cancellation in Form VII set out in the First Schedule.
(3) An authentication service provider who intends to discontinue the provision of authentication products or services to which an accreditation relates shall —

(a) before ceasing to provide an authentication product or service, give the Accreditation Authority at least ninety days’ notice of the intention to discontinue the provision of authentication products and services to which an accreditation relates;

(b) advertise the intention to terminate the accreditation in a daily newspaper of general circulation in Zambia and in such other manner as the Authority may determine;

(c) give all subscribers and holders of each unrevoked or unexpired authentication certificate issued by the authentication service provider at least sixty days’ notice by electronic mail and registered post of the intention to cease acting as an authentication service provider;

(d) ensure that the discontinuation of its operations causes minimal disruption to its subscribers and to persons who require to verify authentication certificates;

(e) make arrangements for the preservation of records in accordance with these Regulations; and

(f) destroy all revoked and expired authentication certificates.

18. An authentication service provider shall not assign, cede or transfer an accreditation to any other person without the prior approval of the Authority.

19. (1) An application to assign, cede or transfer an accreditation shall be made in Form VIII set out in the First Schedule.

(2) The Authority shall —

(a) where it approves an application made under sub-regulation (1), inform the applicant of the approval in Form IX set out in the First Schedule and endorse the approval on the accreditation; or

(b) where it rejects an application made under sub-regulation (1), inform the applicant of the rejection in Form III set out in the First Schedule.

20. (1) An authentication service provider may apply for the renewal of the accreditation in Form X set out in the First Schedule.
21. (1) The Authority may suspend or revoke an accreditation provider an opportunity to be heard, if the accreditation service provider

(2) The Authority shall, where an application complies with the provisions of these Regulations or the conditions of the accreditation, renew the accreditation and endorse the renewal on the accreditation.

(3) The Authority shall, where an application made under sub-regulation (1), inform the applicant of the rejection in Form III set out in the First Schedule and endorse the rejection on the accreditation.
(f) ensure that the authentication service provider issues a report certifying compliance with the prescribed revocation process;

(g) make arrangements for the preservation of records in accordance with these Regulations; and

(h) ensure that the revocation is conducted with minimal disruption to subscribers and relying parties.

(3) Notwithstanding the suspension or revocation of accreditation, the Accreditation Authority may—

(a) take any action necessary to confirm whether the authentication service provider is in breach of any of the requirements, conditions or restrictions subject to which the accreditation was granted;

(b) monitor the progress of the authentication service provider in rectifying the breach;

(c) consider any specific request by the relevant authentication service provider; or

(d) reevaluate its decision to suspend or revoke an accreditation.

(4) If, on the expiration of the period specified in the notice given under sub-regulation (2), and after considering any representations made by the authentication service provider, the Accreditation Authority determines that the accreditation should be suspended or revoked, the Authority may suspend or revoke the accreditation and shall inform the authentication service provider of the suspension or revocation in Form XII set out in the First Schedule.

(5) The Accreditation Authority shall not suspend or revoke an accreditation where its holder takes remedial measures, to the satisfaction of the Accreditation Authority, within such period as the Accreditation Authority may specify.

(6) Where an accreditation is suspended or revoked, its holder shall cease to be entitled to the rights or benefits conferred by, or under, these Regulations with effect from the date of the suspension or revocation and

(a) in the case of a suspension, for the period of the suspension; and

(b) in the case of a revocation, shall surrender the certificate of accreditation to the Authority immediately.

22. (1) The Accreditation Authority shall maintain or cause to be maintained a database of authentication service providers which shall contain—
(a) the details of authentication service providers accredited by the Accreditation Authority;

(b) the names and technical description of the type of authentication product or service provided;

(c) the conditions attached to each accreditation;

(d) the amendment, suspension or revocation of the accreditations;

(e) the descriptions of the accreditation processes, requirements, functions and services of the Accreditation Authority;

(f) the complaints procedure for subscribers to accredited authentication service providers;

(g) the contact particulars of the Authority; and

(j) such other particulars as may be necessary to identify and locate the accreditation service providers or the products or services adequately.

(2) The database referred to in sub—regulation (1) shall be accessible to the public and open for inspection by members of the public at all reasonable times at the offices of the Accreditation Authority.

23. (1) An authentication service provider who is also a certification service provider shall comply with such international standards as may regulate authentication products and services.

(2) An authentication service provider shall issue an authentication certificate to the subscribers in accordance with these Regulations.

(3) An authentication certificate issued by an authentication service provider, which utilises public key infrastructure technology shall, if accredited by the Authority, contain

(a) the serial number of the certificate that distinguishes it from other authentication certificates;

(b) the signature algorithm identifier that identifies the algorithm used by the authentication service provider to sign the authentication certificates;

(c) the name of the authentication service provider that issued the authentication certificate;

(d) the period of validity of the certificate;

(e) the name of the subscriber whose public key the
authentication certificate identifies;
(f) the public key information of the subscriber; and
(g) confirmation that the certificate has been accredited by
the Authority.

(4) An authentication service provider shall, where authentication
products or services utilise public key infrastructure, implement at
a minimum three-factor authentication or a similar level of security
for the storage of the private key.

PART IV
TECHNICAL REQUIREMENTS FOR AUTHENTICATION AND
CERTIFICATION

24. (1) A person who wishes to utilise an authenticated product
or service may apply to the certification Authority or a certification
service provider for an accreditation certificate for use with an
authentication product or service.

(2) A certification service provider shall, upon receipt of an
application under subsection (1)—
(a) establish the identity of the person or entity applying for
an authentication certificate, including physical
identification of the subscriber or authorised key holder;
(b) establish and maintain a verifiable and reviewable process
to confirm that physical identification was undertaken;
and
(c) ensure that the persons performing the physical
identification have undergone appropriate training in
identity and document verification.

(3) A certification service provider shall issue an authentication
certificate to a person or entity that applies for an authentication
certificate upon compliance with the practices and procedures set
forth in the certification service provider’s practice statements,
policies and procedures regarding physical identification of a
prospective subscriber.

(4) A certification service provider shall ensure that an applicant,
authorised person or subscriber is physically present, identified and
accepts the authentication certificate.

(5) A certification service provider shall, where a person relies
on an authentication certificate relating to an authenticated
encryption product or service, be considered to have incorporated
the certification service provider's practice statements, policies and procedures by reference to the certificate.

(6) Where a certification service provider has incorporated a practice statement, policy or procedure into an authentication certificate, the following principles shall apply to the extent that the representations are not inconsistent with the Act or these Regulations:

(a) the certification service provider has complied with all applicable international standards, laws and procedures in issuing the authentication certificate;

(b) where the certification service provider has published the authentication certificate or otherwise made it available to a person who relies on it, the subscriber listed in the authentication certificate has accepted it;

(c) all the information in the authentication certificate is accurate unless the certification service provider states in the authentication certificate that the accuracy of the specified information has not

(d) the certification service provider has no knowledge of any material fact that, if included in the authentication certificate, would adversely affect the reliability of the representations made by the certification service provider; and

(e) where public key infrastructure cryptography is being utilised, that—

(i) the subscriber identified in the authentication certificate holds the private key corresponding to the public key listed in the authentication certificate; and

(ii) the subscribers' public key and private key constitute a functioning key pair.

(7) A certification service provider shall, when conducting an identification or verification of an applicant or subscriber, use the following documents:

(a) where the subscriber or applicant is a natural person, an original valid

(i) national identity document;

(ii) passport; or

(iii) any additional documents as may be necessary to verify identity;
(b) where the subscriber or applicant is a partnership, the constitutive documents of the partnership, if applicable, and the documents referred to in paragraph (a) in respect of each partner in the partnership, including the authorised person or key holder;

(c) where the subscriber or applicant is a company, trust or other legal entity, certified copies of

(i) the relevant constitutive documents;

(ii) a resolution or power of attorney of the directors authorising a specific certification service provider in relation to the issuing, renewal or replacement of certificates; and

(iii) the documents referred to in paragraph (a) in respect of each of the directors, members or trustees of the applicant and the authorised key holder, together with a resolution appointing the representative as the authorised person or key holder.

(8) A certification service provider shall, during the identification of an applicant or subscriber, obtain a handwritten signature from the applicant, authorised person or subscriber on a subscriber agreement.

(9) A subscriber agreement entered into under regulation (7) shall provide that the responsibility for safeguarding the safety of any security device, code or any private key lies with the subscriber.

(10) A subscriber or authorised person shall notify the certification service provider within twenty-four hours if a security device, code or key is lost or compromised.

25. (1) A certification service provider whose authentication product or service is accredited shall make its practice statements, policies and procedures available to the public on its website or in the manner determined by the Accreditation Authority.

(2) A certification service provider whose authentication product or service is accredited shall

(a) at least thirty days before any change is effected to its practice statement, policy or procedure, including changes in—

(i) the identification process;

(ii) the reliance limit of the certificates; or

(iii) key generation, storage or usage;
notify the Authority, the subscribers and third parties of
the intended changes and publish its intention to effect
the changes on its website;

(b) notify the Authority, its subscribers and relying parties by
publication on its website of any incident that adversely
or materially affects or may affect the validity of the
whole or part of its practice statements, policies or
procedures as lodged with the Accreditation Authority;

(c) adhere to its practice statement, policy or procedure when
issuing a type, class or description of authentication
certificates; and

(d) state clearly to its subscribers and interested third parties
all costs and fees related to the issuing, revocation,
suspension, retrieval or verification of the status of an
authentication certificate under each type, class or
description of certificates issued by it.

(3) A certification service provider’s practice statements, policies
and procedures shall, in addition to compliance with international
standards, at a minimum contain the following:

(a) a detailed description of the subscriber identification and
verification process;

(b) provisions governing the conduct of agents, contractors
or other third parties to whom operations have been
outsourced;

(c) clear, detailed and concise provisions for renewal of
authentication certificates;

(d) levels of and reliance limits for, authentication certificates;
and

(e) security device, code or key storage requirements.

26. (1) A subscriber who utilises public key infrastructure
cryptography and whose public key is to be listed in an authentication
certificate issued by the certification service provider, shall generate
a key pair in compliance with the standards prescribed by the
certification service provider or such international standards as may
be applicable.

(2) A subscriber shall provide, in good faith, such information
as the certification service provider may require.

(3) Where a subscriber makes any representations or provides
information to a certification service provider for purposes of
obtaining an authentication certificate, the representations or
information shall be accurate and complete, whether such representations are independently confirmed by the certification service provider or not.

(4) A subscriber shall be considered to have accepted a certificate if the subscriber publishes the certificate in a repository or makes it available to a third party for use.

(5) A subscriber who utilises public key infrastructure cryptography and in whose name an authentication certificate is issued shall be deemed to warrant to all persons who rely on the information contained in the authentication certificate that—

(a) the subscriber rightfully holds the private key corresponding to the public key listed in the authentication certificate;

(b) all the representations made by the subscriber to the certification service provider in relation to the information listed in the authentication certificate are true; and

(c) all the information in the certificate which is within the subscriber's peculiar knowledge is correct.

(6) A subscriber who uses public key infrastructure cryptography shall, on acceptance of an authentication certificate exercise all reasonable care to retain control of the private key corresponding to the public key listed in the authentication certificate and prevent its disclosure to a person not authorised to create the subscriber's advanced electronic signature, during the validity of the authentication certificate, including any period or periods during which the authentication certificate may be suspended.

27. An authentication service provider who is also a certification service provider shall—

(a) utilise a secure and internationally compliant system to perform its services and functions including the—

(i) generation and management of key pairs;

(ii) issuance, renewal, suspension or revocation of authentication certificates; and

(iii) maintenance of a repository and the publication of authentication certificates;

(b) in the event of an occurrence that adversely affects a certification service provider's secure system, use all

Responsibilities of certification service providers
reasonable efforts to notify any person who is or might be affected by that occurrence or act, in accordance with procedures governing response to such an occurrence as specified in its practice statements, policies and procedures;

(c) develop, establish, maintain and update documented policies, procedures and practices in relation to its entire operational environment; and

(d) maintain a publicly accessible database of—

(i) authentication certificates that contain the public keys corresponding to the private keys used by the certification service provider to digitally sign other authentication certificates;

(ii) its certification practice and certificate policy;

(iii) notices of the revocation or suspension of its accreditation;

(iv) any other information relating to an occurrence that adversely affects the reliability of an authentication certificate issued by the certification service provider or the certification service provider's ability to perform its services; and

(v) all accredited authentication products or services.

28. (1) An authentication or certification service provider shall maintain the following records for a period of not less than seven years from the date that they are made:

(a) applications for authentication certificates;

(b) registration and verification documents for authentication certificates;

(c) authentication certificates, stored in a format—

(i) which does not permit an unauthorised person to alter the authentication certificates;

(ii) in which it is possible to verify that the information is correct; and

(iii) in which the authentication certificate is available to the public only where that is expressly permitted by the subscriber;
(d) information related to suspended, expired or revoked authentication certificates;

(e) records and logs for activities that are fundamental to the authentication service provider’s operations, such as certificate management, key generation and administration of computing facilities.

(2) An authentication service provider who is not accredited shall maintain a repository in such a manner that subscribers and relying parties can readily access records to which the authentication service provider permits access in accordance with the Act.

(3) An authentication service provider shall keep information and records in such a manner as to ensure the security, integrity and accessibility of the information and records for purposes of their retrieval and inspection by the Authority.

(4) An authentication service provider shall resign or otherwise revalidate all archived records to protect their integrity and reliability in the event of technological advances that might impact on the reliance that may be placed on the original records.

(5) Where an authentication service provider or a certification service provider’s authentication products or services are based on public key infrastructure cryptography, authentication certificates shall be resigned in accordance with the key lengths specified in the practice statement, policies or procedures.

29. (1) A certification service provider shall, unless the certification service provider and a subscriber agree otherwise, suspend an authentication certification immediately upon receiving a request to do so from the subscriber listed in the authentication certificate or a person duly authorised to act for the subscriber.

(2) A certification service provider shall revoke an authentication certificate—

(a) after receiving a request, upon confirmation that the person requesting the revocation is the subscriber, an agent or otherwise authorised by the subscriber;

(b) after receiving documentary proof of death of a subscriber; or

(c) in the case of a subscriber which is a body corporate, upon presentation of documentary proof that the body corporate has been wound up or otherwise ceased to exist.
(3) A certification service provider shall revoke an authentication certificate where it verifies that—

(a) a material fact represented in the authentication certificate is false;

(b) a requirement for the issuing of the authentication certificate was not satisfied;

(c) the certification service provider's private key or secure system was compromised in a manner that adversely affects the reliability of the authentication certificate; or

(d) a subscriber has breached a subscriber agreement with the certificate service provider.

(4) Where a certification service provider revokes an authentication certificate, it shall immediately notify the subscriber listed in the revoked authentication certificate and publish the revocation in its repository.

(5) A certification service provider shall, not more than twenty-four hours after the suspension or revocation of an authentication certificate, publish a signed notice of the suspension or revocation in the repositories specified in the authentication certificate for publication of notices.

30. (1) An authentication service provider and a certification service provider shall adhere to such international standards as may be notified by the Authority in the Gazette or on its website.

(2) An authentication service provider shall undergo such periodic risk assessments, audits and evaluations as the Accreditation Authority may require in order to ensure compliance with these Regulations or any other written law.

(3) An accreditation granted by the Accreditation Authority is subject to the condition that an authentication or certification service provider shall, on at least five days' written notice, allow the Authority or an auditor appointed by the Authority, as the case may be, to enter its business premises during normal business hours for purposes of audits, and shall upon request, make available for inspection any relevant books, records, supporting documents and other documentation and shall disclose all the information requested by the Authority or auditor and provide all support necessary to conduct the audit.

31. The Accreditation Authority may recognise the accreditation or recognition granted to an authentication or certification service provider or its authentication products or services in any foreign jurisdiction, where the Accreditation Authority is satisfied that such accreditation complies with the provisions of these Regulations.
PART V

PROTECTION OF CRITICAL DATABASE

32. The following databases are hereby declared as critical databases for the purposes of these Regulations:

(a) databases belonging to a public body;

(b) databases belonging to operators of electronic communications networks and the providers of electronic communications services;

(c) databases belonging to institutions whose computer networks are interconnected through external electronic communications networks;

(d) databases belonging to institutions that carry out automated processing of their customers' personal information within the framework of the services they provide through electronic communications technologies networks; and

(e) databases used in connection with public services, including

(i) provision of essential and emergency response services;

(ii) aviation;

(iii) defence and national security;

(iv) law enforcement;

(v) public health and safety;

(vi) banking and financial services; and

(vii) transport and communications.

33. (1) A person who owns, controls or maintains a database which falls within a category referred to in regulation 32 shall cause the database to be registered with the Authority.

(2) The Authority may assess the databases of various persons in order to identify critical databases in accordance with this Part.

34. (1) Where a database is designated as a critical database under this Part, the owner or person in control of the database shall implement effective measures for—

(a) the physical security of the hardware and other infrastructure where the database is located;

(b) limitation of access by persons to the database or information stored in the database;

(c) periodic maintenance and security testing.
(d) timely and uninhibited access to the database by authorised persons;

(e) administrative control of personnel having access to various components of the database;

(f) limitations on use of removable storage devices; and

(g) technical security and disaster recovery.

(2) A person in control of a critical database shall incorporate the measures referred to in sub-regulation (1) into written institutional policies, procedures and codes of practice.

35. (1) A person in control of a critical database shall not permit the integration of the database with a database belonging to a third party where the person does not have in place measures to ensure that the security of the database is not compromised or is likely to be compromised by integration of the database with the database of a third party.

(2) A person in control of a critical database shall, where that person provides public access to the critical database, limit the ability of persons accessing the database to make any alterations to the data or a function connected with the operation of the database.

(3) A person in control of a critical database shall not, without lawful authority, transfer information from a critical database to another database or storage medium or cause to be copied or otherwise structured, information contained in a database.

36. (1) A person in control of a critical database shall implement measures to ensure that a building, room or other structure in which a critical database is located has—

(a) no accessibility to unauthorised persons;

(b) sufficient ventilation to prevent overheating of equipment; and

(c) equipment to prevent or mitigate the effect of a fluctuation of an electric load.

(2) A person in control of a critical database shall ensure that a building, room or other structure is not used for general storage of any material that is not connected to the operation or maintenance of the database.

(3) A person in control of a critical database shall develop a system of security clearance levels for personnel and third parties who have access to a critical database.

(4) A person in control of a critical database shall maintain a register of persons having access to a critical database specifying—
(a) the name and residential address of the person;
(b) the designation of the person within the institution;
(c) the extent of the authorisation and restrictions applicable to the person in relation to utilisation of the database;
(d) the extent to which access to the database by third parties is a pre-condition for access by the person to the database; and
(e) the general level of security clearance a person enjoys in relation to a critical database.

37. (1) A person may, where data stored in a critical database is no longer immediately required for use, place the data in an archive for storage.
(2) Where data has been stored in an archive, the same security requirements, policies, procedures and codes of practice that apply to critical databases shall apply to archived data.
(3) A person shall keep a register of all data that has been archived stating the date on which the data was archived and the persons authorised to access the archived data.

38. (1) A person in control of a critical database shall back up all critical data on a site independent from the location of the critical database.
(2) A backup of data created under sub-regulation (1) shall be stored in such format as to permit the retrieval of data and restoration of the database in the event of the compromise or destruction of the database.

39. (1) A person that is in control of a database shall cause a risk assessment of the institution to be carried out based on the following main elements:
(a) evaluation of organisational security policies, procedures and codes of practice and the structuring of the security function of the institution;
(b) evaluation of the methodology applied in management of the security procedures and the availability of tools to ensure security of the computer system and of the mode of utilising the tools;
(c) technical analysis of the security of all components of the computer system by conducting system integrity tests to ensure system resistance to all kinds of dangers; and
(d) analysis and evaluation of dangers that could result from operating with any deficiencies discovered during the risk assessment exercise.

(2) A risk assessment exercise may be carried out by the Authority or any other person qualified in risk assessment and in particular, assessment related to electronic communications networks, apparatus and services.

(3) A person carrying out a risk assessment exercise shall, at the conclusion of the exercise, deliver to the person concerned a report verified under the hand and seal, where applicable, of that person, confirming the completeness and correctness of the report.

(4) A report submitted to a person under sub-regulation (3) shall contain—

(a) a description and complete evaluation of the security of the computer system, including the measures adopted since the previous risk assessment, if any, and the deficiencies observed in the implementation of recommendations;

(b) a detailed analysis of the organisational and technical deficiencies regarding the security procedures and tools adopted including an evaluation of the risks that could result from operating with the deficiencies discovered; and

(c) proposed organisational and technical security solutions to be adopted in order to overcome the shortcomings noted.

(5) A person in control of a critical database shall cause a risk assessment of the institution to be carried out at least once every twelve months.

(6) The Authority may extend the period referred to in sub-regulation (5), where there are special circumstances that require the extension of the stipulated period, upon a request from a person, in writing, submitted not less than ninety days before the deadline for the conduct of the risk assessment exercise.

(7) A person shall, not later than ten days after the receipt of the risk assessment report, submit a copy of the report to the Authority by such means as the Authority may specify and the Authority shall acknowledge receipt of the report within ten days.

(8) The Authority may, after studying the risk assessment report, request the evaluated person to provide the Authority with further
information, and may carry out an inspection of the institution for the purposes of verification of the matters contained in the risk assessment report.

(9) The Authority may reject a risk assessment report where

(a) the risk assessment is carried out in contravention of these Regulations or any other stipulated procedures; or

(b) the risk assessment report does not contain material information regarding the deficiencies identified by the exercise.

PART VI
INTERCEPTION OF ELECTRONIC COMMUNICATIONS

40. (1) An electronic communications network or service provider shall—

(a) provide an electronic communications service which is capable of being intercepted; and

(b) store electronic communication related information, in accordance with the provisions of the Act and these Regulations.

(2) An electronic communications network or service provider shall—

(a) provide an electronic communications service in respect of which the packets or inband signals of all indirect communications can be duplicated and routed to the Monitoring Centre; and

(b) apply software or apparatus in its electronic communications network or service to duplicate and route to the Monitoring Centre all indirect communications, in consultation with the Monitoring Centre.

(3) An officer authorised by the Monitoring Centre may be stationed at an office or facility of an electronic communications network or service provider for the purpose of facilitating compliance by the electronic communications service provider with the Act and these Regulations.

(4) An electronic communications network or service provider that wishes to put in place measures to ensure compliance with this Part shall, before implementing any service specific solutions, present the proposed solutions to the Monitoring Centre for approval.
41. (1) Where an interception of communication order or a request is presented or made to an electronic communications network or service provider, the provider shall immediately comply with the order or request.

(2) An electronic communication network or service provider shall, in accordance with an interception of communications order or request ensure that —

(a) the entire content of an indirect communication associated with a target identity can be intercepted during the entire interception period; and

(b) any content of an indirect communication associated with a target identity, which is routed to technical storage facilities or is retrieved from such storage facilities can be intercepted during the entire interception period.

(3) An electronic communications network or service provider shall provide the ability to intercept indirect communications in respect of all interception targets utilising its electronic communications network or service and in respect of all target services.

(4) An electronic communications network or service provider shall ensure that all results of an interception of an indirect communication provided at the handover interface shall be uniquely identifiable in relation to the interception of communications order or request through the use of separate channels or unique identifiers.

(5) The interception of the indirect communications shall, after an interception of communications order or a request has been presented to an electronic communications service provider, be conducted in accordance with the interception of communications order or request and any indirect communication that does not fall within the scope of the interception of communications order or request shall be excluded.

(6) An electronic communications network or service provider shall, in relation to each interception target, duplicate and route the signals and packets of each indirect communication.

42. (1) The Monitoring Centre shall, in cooperation with an electronic communications network or service provider ensure that an interception is implemented and operated in such manner that the communicating parties or unauthorised persons cannot detect any change in the communication when an interception is taking place.
(2) The Monitoring Centre shall ensure that during an interception
   (a) the operating facilities of the target service are not altered
       as a result of any interception measure; and
   (b) the operating facilities of any other service are not altered
       as a result of any interception measure.

(3) The Monitoring Centre shall ensure that during an interception
   (a) the quality of service of the target service is not altered as
       a result of any interception measure; and
   (b) the quality of service of any electronic communications
       service other than the target service is not altered as a
       result of any interception measure.

(4) The Monitoring Centre or an electronic communications
    network or service provider shall not provide or otherwise make
    available to an unauthorised person, information on the manner in
    which interception measures are implemented in an electronic
    communications network or target identities and target services to
    which interception is being applied.

(5) An electronic communications network or service provider
    shall keep confidential the manner in which interception measures
    are implemented in an electronic communications apparatus.

(6) A manufacturer of a technical installation for the
    implementation of interception measures in an electronic
    communications apparatus shall keep confidential the manner in
    which interception measures are implemented.

43. (1) The Monitoring Centre and an electronic communications
    network or service provider shall exercise due care in operating
    electronic communications networks in order to ensure that the
    technical arrangements required within an electronic
    communications network to allow interception measures are
    implemented, particularly with respect to—

   (a) protection of information on which and how many target
       identities are or were subject to interception and the
       periods during which the interception measures were
       active;

   (b) restriction to a minimum of staff engaged in implementation
       and operation of an interception measure;

   (c) ensuring the clear delimitation of functions and
       responsibilities and the maintenance of thirdparty
       electronic communications privacy;
(d) ensuring that interception is carried out in operating rooms accessible only by authorised personnel;

(e) the delivery of results of interception delivered through a handover interface to the Monitoring Centre;

(f) restriction of access to information relating to interception;

(g) taking measures to protect the handover interface against misuse;

(h) verification of authorisation for the taking of any action related to interception under this Part;

(i) policies, procedures and codes of practice for authentication and proof of authentication of interception measures;

(j) ensuring that where switched lines to the Monitoring Centre are used, call setup is restricted through the use of closed user group facilities; and

(k) circumstances under which interception measures may require the use of encryption or other confidentiality measures to protect the routing of the results of such interception and cooperation in implementation of encryption or other confidentiality measures.

(2) In order to prevent or trace misuse of the technical functions integrated in the electronic communications network or service enabling interception, any activation or application of the functions in relation to a given identity shall be fully recorded, including any activation or application caused by a faulty or unauthorised input, and the records shall cover—

(a) the target identities of the target service or target services concerned;

(b) the beginning and end of the activation or application of an interception measure;

(c) the result of interception which is routed to the Monitoring Centre;

(d) an authenticator suitable to identify the operating staff, including date and time of input; and

(e) a reference to the interception of communication order or request.

(3) An electronic communications network or service provider shall take reasonable steps to ensure that the records referred to in this regulation are secure and only accessible to authorised persons.
44. (1) An electronic communications network or service provider shall ensure that a technical handover interface or archive provides the results of interception for the entire duration of an interception measure.

(2) An electronic communications network or service provider shall ensure that a handover interface or archive is configured in such a manner, as applicable, to ensure that—

(a) the quality of service of the electronic communications traffic provided at the handover interface or archive is not inferior to that offered to the target service for each particular call;

(b) the routing to the Monitoring Centre of the result of an interception provided at the interface or any required archived data can be implemented with industry standard transmission paths, protocols and coding principles;

(c) each interception target is uniquely associated with a single instance of the handover interface or archive;

(d) there exists a unique correlation between the indirect communication and communication related or archived information;

(e) checksum information on the results of interception is recorded, during the period specified within the interception of communication order or request;

(f) there is ability to route the intercepted indirect communications to the Monitoring Centre through a secure tunnel over circuit or packet switched connections;

(g) the content of an indirect communication routed to the Monitoring Centre includes both incoming and outgoing content;

(h) the arrangements made in an electronic communications network, service or apparatus for the technical implementation of interception measures is set up and configured so as to enable the identification and elimination, without undue delay, of obstacles and potential obstacles in a regional or functional part of that system when several interception measures are operated simultaneously; and

(i) the operating facilities of the target service are not be altered as a result of any interception measure and the operating facilities of any other service are not be altered as a result of any interception measure.
(3) An electronic communications network or service provider shall ensure that the electronic communications network or service provider is able to route the intercepted indirect communications or archived data to the Monitoring Centre via fixed, switched or other applicable connections.

(4) The content of an indirect communication provided across a handover interface or archive shall be in a format that ensures that the content of communications relating to two or more communicating parties—

(a) is placed in a single electronic communications channel;

(b) is placed in two separate electronic communications channels; or

(c) utilises such configurations as are appropriate to the target service concerned.

(5) An electronic communications network or service provider shall, in relation to intercepted indirect communications or archived data, inform the Monitoring Centre immediately of

(a) the activation of an interception measure;

(b) the de-activation of the interception measure;

(c) any change of the interception measure; or

(d) the temporary unavailability of the interception measure due to fault on the network of the electronic communications service provider because of—

(i) link failure or faults on the electronic communications network service provider’s side of the link;

(ii) the temporary unavailability of the interception measure due to software or hardware failure within electronic communications equipment supporting the interception measure; and

(iii) the temporary unavailability of the interception measure due to infrastructure failure resulting from a virus or denial of service attack on an electronic communications network or service.

(6) An electronic communications network or service provider shall ensure that the configuration of the electronic communications network, service or archive can implement and operate each interception measure without or with minimal intervention of third parties.
(7) An electronic communications network or service provider shall, where the electronic communications network or service provider makes use of any electronic communications network, service or archive belonging to a third party, cooperate with the third party in the provision of interception.

(8) Where an interception or archived data duplication measure requires the cooperation of two or more electronic communications network or service providers, a law enforcement officer shall serve an interception of communications order, warrant or request upon each respective electronic communications network or service provider.

(9) An electronic communications network or service provider shall monitor the electronic communications service provider’s capacity in respect of

(a) simultaneous interceptions; and

(b) ability to upgrade any regional or functional part of their electronic communications network or service within a reasonable period of time.

45. (1) The Monitoring Centre shall ensure that an electronic communications network or service provider involved in the implementation of an interception measure, whether alone or in cooperation with a third party, is given no more information relating to operational activities than is strictly necessary to allow the implementation of an interception measure.

(2) An electronic communications network or service provider shall, where the duplication or routing to the Monitoring Centre of signals or packets of an indirect communication is not possible under the circumstances, duplicate or route the remainder of the results of an interception measure to the Monitoring Centre.

(3) Where the special properties of a given electronic communications network or service and the requirements of the Monitoring Centre necessitate the use of various identifying characteristics for determination of the indirect communications to be intercepted, an electronic communications network or service provider shall ensure that the indirect communications can be intercepted on the basis of identifying characteristics as are applicable including—

(a) a physical or postal address;

(b) a telephone number;

(c) a subscriber number;
(d) Mobile Subscriber Integrated Service Digital Network (MSISDN) number;
(e) International Mobile Equipment Identity (IMEI) number;
(f) International Mobile Subscriber Identity (IMSI) number;
(g) a user name;
(h) a subscriber name;
(i) an electronic mail address;
(j) an access login user name;
(k) a session initiation protocol (SIP) uniform resource identifier (URI); or

(j) an Internet Protocol (IP) address and time stamp.

4. The characteristics referred to in sub-regulation (3) shall be identifiable without unreasonable effort and shall allow clear identification of an interception target.

5. An electronic communications network or service provider shall—

(a) ensure that an interception measure implemented pursuant to more than one interception of communications order or request can be applied in respect of one and the same interception target; and

(b) take reasonable precautions to safeguard the identities of the law enforcement agencies concerned so as to ensure the confidentiality of the investigations.

6. An electronic communications network or service provider shall ensure that the indirect communications of at least one in every ten thousand customers, and in the case of an internet service provider, at least two in every twenty-five thousand individual customers and at least one in five hundred of corporate customers can be intercepted simultaneously at any given time by the electronic communications network or service provider and all the results of interception routed to the Monitoring Centre.

7. An electronic communications network or service provider shall ensure that an interception measure can be implemented with reasonable measures to cater for the concurrent operation of several interceptions.

46. (1) An electronic communications network or service provider that is required to implement an interception measure shall provide an electronic communications service in respect of which
all realtime and archived communication related information can be securely—

(a) routed to the Monitoring Centre; or

(b) provided to a law enforcement agency.

(2) The electronic communications network or service provider referred to in sub-regulation (1) shall ensure that realtime or archived communication related information can immediately, on receipt of an interception of communication order or a request, be—

(a) duplicated and routed to the Monitoring Centre; or

(b) provided to the law enforcement agency.

(3) An electronic communications service provider shall, after an interception of communication order or a request is presented to an electronic communications service provider, route or provide realtime or archived communication related information in accordance with the order or request.

(4) Where an electronic communications network or service provider cannot immediately route realtime communication related information to the Monitoring Centre due to a fault on the electronic communications network or service, the electronic communications network or service provider shall buffer the information until it can be routed.

(5) Where—

(a) both a realtime communication related request and an interception of communications order or request, in respect of the same target identity, are received; or

(b) an interception of communication order or request or a realtime communication related request or order that requires information in respect of a future period of time is received;

an electronic communications network or service provider shall ensure capability to route or provide the realtime communication related information in accordance with the interception of communications order or request concerned where

(i) a setup is attempted and a link, data packet transfer or call control session is established with the controlling network element;

(ii) a connection is established;

(iii) no successful connection is established but a
link has been established with the controlling network element;
(iv) a change of service or service parameter occurs;
or
(v) a change of location during an established call occurs.

(6) Where an electronic communications network or service provider is required to route realtime or archived communication-related information to the Monitoring Centre, the electronic communications network or service provider shall ensure capability to route the following realtime or archived communication-related information to the Monitoring Centre for connections originating from, and originating in, the electronic communications network or service provider's electronic communications network or service and terminating or connecting to the target identity as applicable:

(a) destination of an outgoing communication by the target identity including a telephone number, forwarding call number, Mobile Subscriber Integrated Service Digital Network (MSISDN) number, Access Point Name (APN) or Internet Protocol (IP) address;

(b) in relation to a short messaging service, the destination of an outgoing communication by the target identity where receipt of the message is confirmed by the controlling network element, short message service centre (SMSC);

(c) telephone number, Mobile Subscriber Integrated Service Digital Network (MSISDN) number or Internet Protocol (IP) address of originating and intermediate parties of a terminating or connecting communication to the target identity;

(d) the date, time of start and duration of the communication, where available;

(e) the supplementary services or facilities used in association with the connection including three party conference, call diversion, immediate abbreviated dialing, voice mail, facsimile, data and voice;

(f) telephone, subscriber, International Mobile Subscriber
Identity (IMSI), and International Mobile Equipment Identity (IMEI) number of a target identity;

(g) type and nature of communication such as fax, voice or data including incoming, outgoing, link through, intermediate or conference;

(h) intermediate numbers or connections where a target identity establishes conference calls, multiple user connections or calls to link through services or target identities, whether or not at the start of an indirect communication;

(i) multiparty or multiway communications, if and as long as the target identity participates in the multiparty or multiway communications;

(j) identification of the electronic communications apparatus including base stations, terminals and cells that were used to connect or link the target identity at the start of an indirect communication;

(k) data volume, where available;

(l) unstructured supplementary service data (USSD) and universal mobile telephone service (UMTS) data; and

(m) such other data as may be generated by the network or service in connection with an interception measure.

(7) An electronic communications service provider shall comply with the requirements of sub-regulation (6) in relation to outbound connections, links or roaming where the target identity connects, links or roams on a foreign network, where it is possible and practicable to do so.

(8) An electronic communications network or service provider shall record and store the realtime communication related information required by this regulation whenever a call is established.

(9) Where a realtime communication related order or request that requires information that is already available in the records of an electronic communications network or service provider is received, that electronic communications network or service provider shall be capable of immediately routing or providing the real time communication related information under these Regulations in accordance with the order or request concerned.

47. (1) An electronic communications network or service provider shall ensure that the realtime or archived communication related information required to be maintained under these Regulations is immediately available in the records of the

Availability, storage, archival etc. of real time communication related information
(2) An electronic communications network or service provider shall store real-time or archived communication-related information in a format that allows for the extraction of the relevant requested information, in a readable, intelligible and understandable format or in accordance with an order or request.

(3) An electronic communications network or service provider shall, where real-time communication-related information is transferred to an archive or storage facility, ensure that—

(a) all the information is transferred;

(b) the information is not deleted before the expiry of ninety days from the date on which the indirect communication to which the real-time communication-related information relates, is archived; and

(c) the integrity of the information is not compromised.

48. (1) An electronic communications network or service provider shall not avail any real-time or archived communication-related information or information on the manner in which storage measures in respect of real-time or archived communication-related information are implemented to unauthorised persons.

(2) An electronic communications network or service provider shall agree on confidentiality in the manner in which storage measures in respect of real-time or archived communication-related information are implemented with the manufacturers of its technical installations for the implementation of storage measures.

(3) An electronic communications network or service provider shall ensure that the technical arrangements required to allow implementation of the storage measures in respect of real-time or archived communication-related information, are realised with due care exercised in operating electronic communications networks or apparatus, particularly with respect to—

(a) the protection of information on which and how many target identities are or were subject to a real-time communication-related request or order and the periods in respect of which the requests or orders were applicable;
(b) the restriction, to a minimum, of staff engaged in implementation and operation of storage and archival measures in respect of realtime communication-related information;

(c) clear delimitation of functions and responsibilities and the maintenance of thirdparty electronic communications privacy, storing facilities in respect of realtime communication-related information shall be accessible only by authorised personnel;

(d) delivery of realtime or archived communication-related information through a handover interface to the Monitoring Centre or provision to a law enforcement agency;

(e) denial of any form of access to the handover interface or archive by unauthorised persons;

(f) the taking by an electronic communications service provider of necessary measures to protect the handover interface or archive against misuse;

(g) realtime or archived communication-related information being routed to the Monitoring Centre as indicated in the interception of communication order when proof of the authority of the Monitoring Centre to receive, and proof of the authority of the interface to send, has been furnished;

(h) subject to any other written law, implementation of authentication and proof of authentication as agreed upon by the Monitoring Centre and the electronic communications network or service provider;

(i) restriction of call setup through the use of closed user group (CUG) facilities where switched lines to the Monitoring Centre are used;

(j) in appropriate cases, the use, by an electronic communications network or service provider, of encryption or other confidentiality measures to protect the routing of realtime or archived communication-related information that the Monitoring Centre or law enforcement officers may require;

(k) the capability of an electronic communications network or service provider's handover interfaces and archives to support the use of encryption, authentication, integrity
checking or other confidentiality measures; and

(l) cooperation with law enforcement agencies or the
    Monitoring Centre, or a person authorised by them, to
    implement encryption, authentication, integrity checking
    or other confidentiality measures as may be required.

(4) An electronic communications network or service provider
    shall, in order to prevent or trace misuse of the technical functions
    integrated in the electronic communications network, service or
    apparatus enabling the storing, routing and provision of real time or
    archived communication related information, record any activation
    or application of a function in relation to a target identity, including
    any activation or application caused by faulty or unauthorised input.

(5) A record maintained pursuant to sub-regulation (4) shall
    include information on—

(a) the target identities of the target service or target services
    concerned;

(b) the beginning and end of the activation or application of
    the real time communication related request or order or
    archived communication related information;

(c) the Monitoring Centre to which the real time or archived
    communication related information is routed or law
    enforcement agency to which it is provided;

(d) an authenticator, including date and time of input, suitable
    to identify the operating staff; and

(e) a reference to the order or request.

(6) An electronic communications network or service provider
    shall take reasonable steps and implement reasonable measures to
    ensure—

(a) that the records maintained under sub-regulation (5) are
    secure and only accessible to specific authorised persons;

(b) the integrity of real time or archived communication related
    information when it is recorded or stored;

(c) the physical, environmental and logical security of all stored
    and archived real time communication related information; and

(d) availability of real time and archived communication
    related information.
49. (1) An electronic communications network or service provider shall ensure that a technical handover interface or archive provides all the requested realtime or archived communication-related information in a readable, intelligible and understandable format, and in accordance with the request or order.

(2) The configuration of the handover interface or archive referred to in sub-regulation (1) shall be such that—

(a) the routing to the Monitoring Centre of the requested realtime or archived communication-related information provided at the interface can be implemented using standard, generally available transmission paths, protocols and coding principles;

(b) each instance of requested realtime or archived communication-related information is uniquely associated with a single instance of the handover interface;

(c) the format for routing the requested realtime or archived communication-related information to the Monitoring Centre is implemented with an industry standard format;

(d) an electronic communications network or service provider is able to route or provide the requested realtime or archived communication-related information to the Monitoring Centre; and

(e) the associated storage system can store, maintain, extract, process, transmit or provide realtime communication-related information with minimum or no involvement of third parties.

(3) An electronic communications network or service provider shall inform the Monitoring Centre of—

(a) any change of the handover interface, storage system, measures and functionality that may impact on the routing, provision or configuration of realtime or archived communication-related information; and

(b) the temporary unavailability of stored realtime or archived communication-related information.

(4) Where an electronic communications network or service provider uses any third party electronic communications network or service provider's network or service or a storage provider's service, the electronic communications service provider or any other electronic communications network or service provider or storage provider shall cooperate in the storing, routing or provision of
realtime or archived communication-related information.

(5) An electronic communications network or service provider shall ensure that—

(a) any third party electronic communications network or service provider or storage provider involved in the storing, provision or routing of realtime or archived communication-related information is given no additional information relating to operational activities than is strictly necessary to facilitate the storage, provision or routing of realtime or archived communication-related information; and

(b) any third party electronic communications network or service provider or storage provider involved in the cooperative storing, provision or routing of realtime or archived communication-related information is given no additional information relating to operational activities than is strictly necessary to allow the storage, provision or routing of realtime or archived communication-related information.

(6) Where the provision or routing of requested realtime communication-related information under these Regulations is not possible, the remainder of the realtime communication-related or archived information shall nevertheless be provided to the law enforcement agency or routed to the Monitoring Centre.

(7) An electronic communications network or service provider shall ensure that storage devices or media shall be clearly indexed or the information contained identified to ensure the retrieval of only requested real time communication information without unreasonable effort or delay.

(8) An electronic communications network or service provider shall ensure that only one request or order for realtime communication-related information can be operated concurrently for one and the same storage device or media.

(9) An electronic communications network or service provider shall, where one or more requests or orders for realtime or archived communication-related information are processed, take reasonable precautions to safeguard the identities of the law enforcement agencies and ensure the confidentiality of the investigations and information.

(10) An electronic communications network or service provider shall ensure that the archived communication-related information
can, within the period specified in the request or order, be duplicated, processed and routed to the Monitoring Centre or provided to a law enforcement agency in accordance with the request or order.

50. An electronic communications network or service provider shall store realtime or archived communication-related information for a period of ten years from the date on which the indirect communication to which the communication-related information relates, is recorded or archived, as the case may be.

PART VII

DETAILLED SECURITY, FUNCTIONAL AND TECHNICAL REQUIREMENTS FOR INTERCEPTION

51. (1) An electronic communications network or service provider shall implement measures to ensure implementation of functionality and security of the facilities and apparatus to make the electronic communications network or service provider’s network or service compliant with lawful interception requirements.

(2) An electronic communications service provider shall implement—

(a) a marking facility for lawful interception compliance purposes; and

(b) a mediation device for the collection from network elements, normalisation and delivery to the Monitoring Centre of interception related information (IRI) tickets in the format referred to in a specified standard; which shall comply with the physical and access control security measures as may be specified in these Regulations.

(3) An electronic communications network or service provider shall, within a marking facility, implement an Interception Management System (IMS) which is protected from the rest of the electronic communications network or service provider’s network by means of one or more network firewalls, composed of one or more lawful interception servers and one or more administration workstations, for the marking and management of targets and interceptions.

(4) Where an electronic communications network or service provider operates a public switched telecommunications network, fixed line network or mobile communications network, the interception management system referred to in sub-regulation (3) shall—
(a) where necessary, utilise mediation devices for the collection from network elements, normalisation and delivery to an interception centre, of interception related information, and tickets in the format specified in these Regulations; and

(b) implement the Internal Interception Function (IIF), of network elements, when provided by the vendor and shall be used in preference to physical wiretap and external interception equipment.

(5) Where external interception equipment is necessary as a result of the non-provision of an internal interception function by a vendor, the interception function shall be implemented in dedicated hardware or firmware and shall be connected in a manner that shall not disrupt the normal operation of the electronic communications network when the apparatus fails.

(6) Where an electronic communications network or service provider operates a public switched telecommunications network, fixed line network or mobile communications network, the marking facility implementation for lawful interception purposes shall comply with the standards prescribed under these Regulations and may, in addition comply with the Communications Assistance for Law Enforcement (CALEA) J STD 025 standard.

(7) A dedicated area of the marking facility shall conform to the physical security requirements stipulated in a prescribed standard.

(8) A physical access control system shall be applied to the marking facility and shall—

(a) be implemented using an electronic access control device; and

(b) provide detailed logs of both successful and failed access attempts to the facility.

(9) An electronic communications network or service provider operating a public switched telecommunications network, fixed line network or mobile communications network shall only use a mechanical key mechanism in the event of the electronic access control device or the access control system failing and the key shall be kept safely with strict control over its access.

(10) An electronic communications network or service provider operating a public switched telecommunications network, fixed line network or mobile communications network shall, at a minimum, implement a logical access control to the marking
facility using a token-based authentication mechanism such as a digital certificate enabled smart card, onetime password token or radio frequency identification (RFID) token.

(11) A logical access control system shall, as far as is possible, on the provisioning and mediation platforms at the marking facility, provide detailed logs of both successful and failed access attempts to access these platforms.

(12) The access control systems to the marking facility that provide detailed logs of both successful and failed access attempts to the facility shall be hosted within the marking facility itself and the logs shall be maintained for a period of thirty days.

(13) An electronic communications network or service provider shall ensure that to the extent that the electronic communications network or service provider is obligated to consult on the manner in which interception measures are implemented in a given electronic communications network or apparatus with the designer, manufacturer, distributor, installer or other supplier of such electronic communications network or apparatus for the implementation of interception measures, such consultation shall be subject to confidentiality undertakings by the relevant designer, manufacturer, distributor, installer or other supplier.

(14) An electronic communications network or service provider operating a public switched telecommunications network, fixed line network, internet service or mobile communications network or service shall implement the following minimum functions for which the processes used to support the functions shall be well documented and auditable:

(a) the support of the Monitoring Centre, including provision on request of customer-related targeting information required for inclusion in an interception of communications order or request;

(b) the receipt of lawful interception orders and requests from the Monitoring Centre and law enforcement officers;

(c) the implementation of secure communications measures for delivery of orders or requests including a secure facsimile or electronically signed and encrypted electronic mail or other messaging means determined in conjunction with the Monitoring Centre;

(d) verification of the validity of the warrant, order or request including the telephonic or online verification of the lawful interception identifier (LIID) stipulated in the
interception of communications order or request with the department responsible for Government Communications;

(e) availing of the order, request or direction into the Interception Management System (IMS) according to the targeting and timing information stipulated in the warrant or direction;

(f) the electronic or physical confirmation of the activation of the order, request or direction to the Monitoring Centre through the Interception Management System (IMS);

(g) administration of the physical, logical, lawful interception application and interception management system (IMS) security and access control mechanisms;

(h) systems administration, including configuration management, change management, backup and disaster recovery of the lawful interception servers, databases, mediation devices and workstations implemented in a marking facility;

(i) reports on performance, availability, capacity, utilisation and other measures to the Monitoring Centre;

(j) reporting on security breach attempts and failed access attempts to the department responsible for Government Communications;

(k) routine systems maintenance on the software and hardware implemented in the marking facility;

(l) regular provision of reports available in the lawful interception marking facility to the Monitoring Centre; and

(m) regular internal and external audit of security and operations within a marking facility and management of information security risks associated with providing this facility and capability.

52. (1) An electronic communications network or service provider operating a public switched telecommunications network, fixed line network or mobile communications network shall implement a network security protocol which shall—

(a) ensure that network access to the marking facility is secured through means of a network firewall and, in the case of a mobile communications network or service, based on protocol proxy or stateful protocol inspection technology;
(b) ensure that the rule set on the firewall explicitly denies all externally originated communication sessions unless stipulated otherwise by the Monitoring Centre;

(c) ensure that the firewall security is augmented with intrusion detection systems capable of identifying and blocking network hacking attempts on the marking facility;

(d) regularly update the Intrusion Detection System (IDS) pattern files from the vendor of the intrusion detection system (IDS) solution; and

(e) implement both network and server based antivirus solutions for the marking facility and regularly update the antivirus definition files from the vendor of the antivirus software.

(2) An electronic communications network or service provider operating a public switched telecommunications network, fixed line network or mobile communications network shall ensure that the communication link between the marking facility and the Monitoring Centre for the delivery of interception related information shall be encrypted, at a minimum, using—

(a) an Internet Protocol (IPSec) based link encryption device working in encapsulating security payload (ESP) mode utilising an encryption algorithm of—

(i) 168bit encrypt decrypt encrypt (EDE) mode triple data encryption standard (3DES), in the case of a public switched telecommunications network or fixed line network; and

(ii) 468bit encrypt decrypt encrypt (EDE) mode triple data encryption standard (DES); or

(b) 192bit cipher block chaining (CBC) mode advanced encryption standard (AES).

(3) An electronic communications network or service provider operating a mobile communications network or service shall transmit interception related call content from the mobile communications network to the Monitoring Centre through one or more gateway switches close to the Monitoring Centre through an integrated service digital network (ISDN) link based, at a minimum, on the International Telecommunications Union, Telecommunication Standardisation Sector (ITU-T) Q.931DSS1 or similar standard.
53. (1) An electronic communications network or service provider operating an internet service shall implement the internet service so as to install and maintain lawful interception software, probes and any associated tapping and interception devices, positioned in the internet service provider’s network to ensure that

(a) all network traffic to and from servers hosted by the internet service provider can be intercepted;

(b) all network traffic to and from access authentication servers hosted by the ISP can be intercepted; and

(c) all network traffic originating from or destined for an interception target which is carried across the internet service provider’s network links can be intercepted.

(2) An electronic communications network or service provider operating an internet service shall implement and manage one or more interception provisioning terminals for lawful interception compliance purposes, which shall be sufficiently closely located on the network to the probes or devices being managed by electronic communications network or service providers so as to ensure that a delay in provisioning an interception based on access login information is minimised.

(3) An electronic communications network or service provider operating an internet service shall, where necessary, implement mediation devices for the collection from probes and devices, normalisation and delivery to the Monitoring Centre, of interception related information (IRI) tickets in accordance with these Regulations.

(4) An electronic communications network or service provider operating an internet service shall ensure that interception provisioning terminals are housed in areas with access controls implemented to limit access to authorised staff only and which may be accessible remotely across a network, in which case an encrypted communication channel shall be used.

(5) An electronic communications network or service provider operating an internet service shall ensure that logical access control is implemented on the provisioning terminals, at minimum, using a password that is changed at least once a month.

(6) An electronic communications network or service provider operating an internet service shall ensure that a provisioning terminal and mediation device—

(a) is configured to provide detailed logs of both successful
55. (1) An electronic communications network or service provider operating an internet service shall, as far as is possible, apply specifications relevant to its network from the standards specified in these Regulations and any deviations and option choices from specifications provided in the standards shall be communicated to and agreed upon by the Monitoring Centre prior to implementation.

(2) The standards to be applied by an electronic communications network or service provider under sub-regulation (1) shall be in compliance with the European Telecommunications Standards Institute (ETSI) technical specifications set out in—

(a) TS 102 232 Version 1.1.1 200108: Telecommunications security, Lawful Interception (LI): Handover specification for internet protocol delivery: Technical interface for mediation and handing over of intercepted internet protocol traffic to a Monitoring Centre, including voiceover internet protocol (VoIP);

(b) TS 102 233 Version 1.2.1 200204: Telecommunications security, Lawful Interception (LI): Handover Specification for electronic mail delivery: Technical interface for the mediation and handing over of intercepted electronic mail to a Monitoring Centre; and

(c) TS 102 234 Version 2.5.1 200301: Telecommunications security, lawful interception (LI): Service Specification details for internet access services: Specification of lawful interception (LI) requirements to internet service providers providing an internet access service directly to endusers.

(3) An electronic communications network or service provider operating an internet service shall transmit the result of interception from the internet service provider’s mediation device to the interception centre through a shared or dedicated internet protocol connection over the internet or through a direct circuit to the Monitoring Centre.

(4) Alternative specifications that an electronic communications network or service provider operating an internet service may adopt where the standard referred to in subregulation (2) is not applicable, shall be the latest versions of Communications Assistance for Law Enforcement (CALEA) JSTD025 and transport of intercepted internet protocol traffic (TIT) standards.
56. The fees prescribed in the Second Schedule shall be payable in respect of the matters stated therein.

57. (1) An electronic communications network or service provider shall ensure that they have in place equipment that has the capability to enable interception within six months from the date of coming into operation of these Regulations.

(2) The Monitoring Centre may determine a longer period for the implementation of any provision of these Regulations where there are special circumstances giving rise to the need for a longer duration.
and failed access attempts to the terminal;

(b) is secured through means of a network firewall and the rule set on the firewall explicitly denies all externally originated communication sessions unless they are from the Monitoring Centre; and

(c) has appropriate virus protection in the provisioning terminals and the virus protection chosen should be updated as often as is reasonably possible;

(7) An electronic communications network or service provider operating an internet service shall ensure that the communication link between the mediation device and the Monitoring Centre for the delivery of interception related information and intercepted content shall be encrypted using an Internet Protocol (IPSec) based link encryption software or device working in Encapsulating Security Payload (ESP) mode and utilising an encryption algorithm of either 168bit encrypt decrypt encrypt (EDE) mode triple data encryption standard (DES) or 192bit cipher block chaining (CBC) mode advanced encryption standard (AES) as specified by the Monitoring Centre.

54. (1) An electronic communications network or service provider operating a public switched telecommunications network, fixed line network or mobile communications network shall, as far as is possible, apply specifications relevant to its network from the standards specified to in these Regulations and any deviations and option choices from specifications provided in the standards shall be communicated to, and agreed upon by, the Monitoring Centre prior to implementation.

(2) The standards to be applied by an electronic communications network or service provider under sub-regulation (1) shall be in compliance with the European Telecommunications Standards Institute (ETSI) technical specifications set out—

(a) in the case of a public switched telecommunications network, fixed line network, in

(i) TS 101 331 Version 1.1.1 200108: Telecommunications security, Lawful Interception (LI): Requirements of law enforcement Agencies: LI requirements from a Law Enforcement Agency (LEA) point of view;

(ii) ES 201 158 Version 1.2.1 200204: Telecommunications security, Lawful
(iii) **TS 101 671 Version 2.5.1 200301**: Telecommunications security, Lawful Interception (LI): Handover interface for the lawful interception of telecommunications traffic: Generic flow of information, the procedures, the information elements and the network or service specific protocols relating to the provision of lawful interception at the handover interface; and

(b) in the case of a mobile communications network, in—

(i) specifications for lawful interception: release phase 2+ for Global System for Mobile (GSM) and General Packet Radio Service (GPRS) services;

(ii) specifications for lawful interception in third generation partnership project (3GPP) Release’ 99 for universal mobile telephone service (UMTS);

(iii) **TS 133 106** lawful interception (LI): Requirements for universal mobile telephone service (UMTS);

(iv) **TS 133 107** lawful interception (LI): Architecture and Functions for universal mobile telephone service (UMTS); and

(v) **TS 133 108** lawful interception (LI): Handover Interface for universal mobile telephone service (UMTS).

(3) An electronic communications network or service provider shall ensure that—

(a) a sufficiently current software version release is implemented on all the switching elements to support compliance with these Regulations within the network; and

(b) all of the lawful interception features required for the compliance with these Regulations and implemented in the switching element software are fully installed and enabled.
**APPLICATION TO PROVIDE CRYPTOGRAPHY/AUTHENTICATION SERVICES**

<table>
<thead>
<tr>
<th>Information Required</th>
<th>Information Provided</th>
<th>Certificate code</th>
<th>Licence no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaded fields for official use only</td>
<td>Date</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. **Type of licence (where applicable)**

2. **Type of cryptography or authentication service**

3. **Type of network**

4. **Name(s) of applicant(s)**

5. **Type of applicant**
   - Individual
   - Company
   - Partnership

6. **Notification address**
   - Tel:
   - Fax:
   - E-mail:

7. **Information of contact person authorised to represent the applicant**
   - Tel:
   - Fax:
   - E-mail:

8. Where the applicant is a company, the following details are required:

   - **company name**
8. Have you ever applied to provide cryptography/authentication services in Zambia? If yes please give details:

<table>
<thead>
<tr>
<th>Service applied for</th>
<th>Location</th>
<th>Brief description of service</th>
<th>Date of application</th>
<th>Status of application (Granted, rejected or pending)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(b) * If application was rejected, give reasons for rejection:

10. Service commencement details

<table>
<thead>
<tr>
<th>Proposed commencement date</th>
<th>District</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(b) Brief description

11. Have you been convicted of an offence involving fraud or dishonesty or of any offence under the Electronic Communications and Transactions Act, 2009, or any other law within or outside Zambia? If yes, specify details:

<table>
<thead>
<tr>
<th>Nature of offence:</th>
<th>Date of Conviction:</th>
<th>Sentence:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12. Appendices*

<table>
<thead>
<tr>
<th>Appendix No. 1</th>
<th>Service design, roll-out plan and implementation schedule including coverage area and intended performance levels and services to be outsourced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix No. 2</td>
<td>Technical specifications for interoperability and compatibility of the cryptography service with other systems, including those owned and operated by electronic communications service licensees or in the case of an application for a certificate of accreditation, technical specifications of authentication products or services to be provided.</td>
</tr>
<tr>
<td>Appendix No. 3</td>
<td>Business plan for proposed services (Should include information on technical proposal of the services to be provided, information on previous experience, and the profile of the individual, company or partnership, as the case may be.)</td>
</tr>
<tr>
<td>Appendix No. 4</td>
<td>Certification practice and procedure specifications where the cryptography service provider is also a certification service provider</td>
</tr>
<tr>
<td>Appendix No. 5</td>
<td>Certified photocopies of work permits and other relevant permits issued by the Immigration Department (where applicable) Tax Payers Identification Number (TPIN)</td>
</tr>
</tbody>
</table>

13. QUALITY OF SERVICE UNDERTAKING
I/we declare that the quality of service I/we provide shall meet the minimum requirements set out under the Act or any other law or, guidelines published by the Authority or any international standard.

14. DECLARATION
I/we declare that all the particulars and information provided in this application are complete, correct and true and I/we agree that in the event that any of the said particulars and information provided is found to be untrue or fraudulent, the certificate or registration/accreditation will be revoked.

I/we agree that in the event of the revocation of the certificate or registration accreditation, any fee paid to the Authority for certificate or registration/accreditation shall be forfeited.

I/we declare that in the event that the nature of my/our business changes, or I/we no longer carry out operations in terms of the registration, I/we will notify the Authority in which case my/our registration may be revoked or revised.

Declared at ... this ...... day of .............. 20 ........... by the following persons who are duly authorised to sign for and on behalf of the applicant under the authority of the Power of Attorney or Board Resolution which is hereby attached.

Applicant's name __________________________ Date ______________

Applicant's signature __________________________

FOR OFFICIAL USE ONLY
Received by: __________________________ officer

Date Received __________________________

Amount Received __________________________

Serial No. of application: __________________________ STAMP

RECEIPT No. __________________________
Form II
(Regulations 5 and 15)

ZICTA
ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Electronic Communications and Transactions Act, 2009
(Act No. 21 of 2009)
The Electronic Communications and Transactions (General) Regulations, 2011

CERTIFICATE No.

CERTIFICATE OF REGISTRATION/ACCREDITATION AS CRYPTOGRAPHY OR AUTHENTICATION SERVICE PROVIDER
(Section 22 of the Electronic Communications and Transactions Act, No. 21 of 2009)

Holder’s name
Address

Type of business: provision of the following cryptography or authentication services:
(a)
(b)
(c)
(d)
(e)
(f)
(g)

The certificate is valid from the ....... day of ...... to the ...... day of ............ 20.......

The conditions of grant of the certificate or registration/accreditation are as shown in the Annexure attached hereto.

Issued at .......... this .......... day of ............

------------------------------------------------------------------

Director General

ENDORSEMENT OF REGISTRATION

This certificate has, this .......... day of ............ 20........... been entered in the Register.

------------------------------------------------------------------

Director-General
<table>
<thead>
<tr>
<th>Date of transfer/amendment/variation/renewal</th>
<th>Details of transfer/amendment/variation/renewal</th>
<th>Date of Registration and Registration No.</th>
<th>Signature of Director-General</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Form III

(Regulations 5, 9(2), 10(3), 15, 19(2) and 20(3))

The Electronic Communications and Transactions Act, 2009
(Act No. 21 of 2009) The Electronic Communications and Transactions (General) Regulations, 2011

NOTICE OF REJECTION OF APPLICATION

To (1)..............................................................

of (2)..............................................................

IN THE MATTER OF (3).................................... you are hereby notified that your application has been rejected on the following grounds:

(a)................................................................

(b)................................................................

(c)................................................................

(d)................................................................

Dated this ...................day of ................... 20..................

.................................................................

Director-General

(1) Here insert the full names of applicant
(2) Here insert address of applicant
(3) Here insert the reference No. of application

FOR OFFICIAL USE ONLY

This rejection has, this ................... day of ................... 20 .................., been entered in the Register.

.................................................................

Director-General
Form IV

(Regulation 6(1) and 16(1))

(To be completed in triplicate)

ZICTA
ZIMBABWE INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Electronic Communications and Transactions Act, 2009
(Act No. 21 of 2009)

The Electronic Communications and Transactions (General) Regulations, 2011

NOTIFICATION OF CHANGE IN PARTICULARS

<table>
<thead>
<tr>
<th>Information Required</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licence code</td>
<td>Date and Time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaded fields for official use only</td>
</tr>
</tbody>
</table>


2. Holder

3. (a) Name(s) of applicant(s)
   (b) Type of applicant
<table>
<thead>
<tr>
<th>Individual</th>
<th>Company</th>
<th>Partnership</th>
</tr>
</thead>
</table>

4. (a) Date of Birth (dd/mm/yyyy)
   (b) Nationality
   (c) Identity card (NRC) No. or Passport No. (attach copies)
   | | | |

5. Applicant’s Address
   Tel:
   Fax:
   E-mail:
6. Specific changes

- (a)
- (b)
- (c)
- (d)
- (e)
- (f)

7. Appendix

Copy of minutes of meeting at which decision to change particulars was made.

Applicant

Date

Signature

FOR OFFICIAL USE ONLY

Received by: ______________________

Officer STAMP
<table>
<thead>
<tr>
<th>Information Required</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Type of certificate</td>
<td>Shaded fields for official use only. Tick where applicable. Certificate code.</td>
</tr>
<tr>
<td>2. (a) Name(s) of applicant(s)</td>
<td>Individual Company Partnership</td>
</tr>
<tr>
<td>(b) Type of applicant</td>
<td></td>
</tr>
<tr>
<td>3. (a) Nationality</td>
<td></td>
</tr>
<tr>
<td>(b) Identity card (National Registration Card No. or Passport No.)</td>
<td></td>
</tr>
<tr>
<td>4. (a) Notification Address</td>
<td></td>
</tr>
<tr>
<td>Tel:</td>
<td></td>
</tr>
<tr>
<td>Fax:</td>
<td></td>
</tr>
<tr>
<td>E-mail:</td>
<td></td>
</tr>
<tr>
<td>(b) Information of contact person authorised to represent the applicant</td>
<td></td>
</tr>
<tr>
<td>Tel:</td>
<td></td>
</tr>
<tr>
<td>Fax:</td>
<td></td>
</tr>
<tr>
<td>E-mail:</td>
<td></td>
</tr>
<tr>
<td>5. (a) Company name:</td>
<td></td>
</tr>
<tr>
<td>(b) Company address:</td>
<td></td>
</tr>
<tr>
<td>(c) Company Registration No.</td>
<td></td>
</tr>
<tr>
<td>6. Proposed variations/amendments</td>
<td>(a)</td>
</tr>
<tr>
<td>(b)</td>
<td></td>
</tr>
<tr>
<td>(c)</td>
<td></td>
</tr>
<tr>
<td>(d)</td>
<td></td>
</tr>
<tr>
<td>(e)</td>
<td></td>
</tr>
<tr>
<td>(f)</td>
<td></td>
</tr>
<tr>
<td>(g)</td>
<td></td>
</tr>
<tr>
<td>7. Appendices</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Appendix No. 1 Minutes of company or partnership</td>
<td></td>
</tr>
<tr>
<td>meeting at which decision was made</td>
<td></td>
</tr>
<tr>
<td>Appendix No. 2 Reasons for proposed amendments</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applicant's name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Applicant's signature

FOR OFFICIAL USE ONLY

Received by: ___________________________ Officer ___________________________ RECEIPT No. ___________________________

Amount Received: ___________________________

Serial No. of application: ___________________________ STAMP ___________________________
NOTICE OF INTENTION TO SURRENDER CERTIFICATE OF REGISTRATION/ACCREDITATION

<table>
<thead>
<tr>
<th>Information Required</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Name of holder</td>
<td></td>
</tr>
<tr>
<td>3. Expiry date</td>
<td></td>
</tr>
<tr>
<td>4. Holder’s Address</td>
<td></td>
</tr>
<tr>
<td>Tel:</td>
<td></td>
</tr>
<tr>
<td>Fax</td>
<td></td>
</tr>
<tr>
<td>E-mail:</td>
<td></td>
</tr>
<tr>
<td>5. Reasons for surrender</td>
<td></td>
</tr>
<tr>
<td>6. Appendix</td>
<td></td>
</tr>
<tr>
<td>Record of board meeting at which decision to surrender was made</td>
<td></td>
</tr>
</tbody>
</table>

Applicant __________________________ Date ____________

Officer __________________________ Date ____________

FOR OFFICIAL USE ONLY

Received by: ______________________ Officer ______________________ STAMP

Amount Received: ___________________ Serial No. of application: ___________________
Form VII

(Regulations 7(2)(b)
and 17(2)(b))

ZICTA
ZAMBIA INFORMATION AND COMMUNICATION TECHNOLOGY AUTHORITY

The Electronic Communications and Transactions Act, 2009
(Act No. 21 of 2009)

The Electronic Communications and Transactions (General) Regulations, 2011
NOTICE OF CANCELLATION/LAPSE OF CERTIFICATE OF REGISTRATION/ACCREDITATION

To (1)........................................................................

........................................................................

IN THE MATTER OF (2).............................................. you are hereby notified that pursuant to regulation 7 /regulation 17 your certificate No. (3).................................................. has been cancelled subject to the terms and conditions annexed hereto.

Dated this ........................................ day of 20..........................................................

........................................................................

Director-General

(1) Here insert the full names and address of applicant

(2) Here insert reference No. of application

(3) Here insert certificate No.

FOR OFFICIAL USE ONLY

This notice has, this ................ day of .............. 20 .............. been entered in the Register

........................................................................

Director-General
<table>
<thead>
<tr>
<th>Information Required</th>
<th>Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Certificate No.</td>
<td>licen Code Date/Time</td>
</tr>
<tr>
<td>2. Current holder</td>
<td></td>
</tr>
<tr>
<td>3. (a) Name(s) of assignee(s)</td>
<td></td>
</tr>
<tr>
<td>(b) Details of assignee</td>
<td>NRC No. Passport No.</td>
</tr>
<tr>
<td>(c) Type of assignee</td>
<td>Individual Company Partnership</td>
</tr>
<tr>
<td>4. Assignee’s Address</td>
<td></td>
</tr>
<tr>
<td>Tel:</td>
<td></td>
</tr>
<tr>
<td>Fax:</td>
<td></td>
</tr>
<tr>
<td>E-mail:</td>
<td></td>
</tr>
<tr>
<td>5. Appendices</td>
<td></td>
</tr>
<tr>
<td>Appendix No. 1</td>
<td>Minutes of relevant meeting</td>
</tr>
<tr>
<td>Appendix No. 2</td>
<td>Resolution of relevant meeting</td>
</tr>
<tr>
<td>Appendix No. 3</td>
<td>Reasons for transferring, ceding or assigning</td>
</tr>
</tbody>
</table>

Name of Applicant (individual or authorised company representative):
Date: ______________________ SIGNATURE: ______________________

FOR OFFICIAL USE ONLY
Received by: ______________________ Officer ______________________
Amount Received ______________________ STAMP ______________________
Serial No. of application: ______________________
ZICTA

The Electronic Communications and Transactions Act, 2009
(Act No. 21 of 2009)
The Electronic Communications and Transactions (General) Regulations, 2011

CONSENT TO TRANSFER, CEDE OR ASSIGN CERTIFICATE

To (1)........................................................................................................................................

IN THE MATTER OF (2)........................................................................................................... you are hereby notified that your application for consent to *transfer, cede or assign your Certificate No. (3) ......................................................................................... has been approved.

The conditions of the grant of the consent are shown in the Annexures attached hereto.

Dated this ........................................ day of .................................................. 20..................

.................................................................
Director-General

(1) Here insert the full names and address of licensee
(2) Here insert the application reference No.
(3) Here insert Certificate No.

*Delete as appropriate

FOR OFFICIAL USE ONLY

This consent has, this .............. day of .............. 20............ been entered in the Register

.................................................................
Director-General
Form X

(Regulations 10(1) and 20(1))
(To be completed in triplicate)

ZICTA
ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

The Electronic Communications and Transactions Act, 2009
(Act No. 21 of 2009)
The Electronic Communications and Transactions (General) Regulations, 2011

<table>
<thead>
<tr>
<th>APPLICATION FOR RENEWAL OF CERTIFICATE OF REGISTRATION/ACCREDITATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaded fields for official use only Tick where applicable</td>
</tr>
<tr>
<td>Certificate code Date/Time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Information Required</strong></th>
<th><strong>Information Provided</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Type of Certificate</td>
<td></td>
</tr>
<tr>
<td>2. (a) Name(s) of applicant(s)</td>
<td></td>
</tr>
<tr>
<td>(b) Type of applicant</td>
<td>Individual</td>
</tr>
<tr>
<td>3. (a) Nationality</td>
<td></td>
</tr>
<tr>
<td>(b) Identity card (National Registration Card No. or Passport No.)</td>
<td></td>
</tr>
<tr>
<td>4. (a) Notification Address</td>
<td></td>
</tr>
<tr>
<td>Tel:</td>
<td></td>
</tr>
<tr>
<td>Fax:</td>
<td></td>
</tr>
<tr>
<td>E-mail</td>
<td></td>
</tr>
<tr>
<td>(b) Information of contact person authorised to represent the applicant</td>
<td></td>
</tr>
<tr>
<td>Tel:</td>
<td></td>
</tr>
<tr>
<td>Fax:</td>
<td></td>
</tr>
<tr>
<td>E-mail:</td>
<td></td>
</tr>
<tr>
<td>5. (a) Company name</td>
<td></td>
</tr>
<tr>
<td>(b) Company address</td>
<td></td>
</tr>
<tr>
<td>(c) Company registration No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Previously held certificates in Zambia, if any, by applicant issued under the Electronic Communications and Transactions Act, 2009</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>(a)</td>
</tr>
<tr>
<td></td>
<td>(b)</td>
</tr>
<tr>
<td></td>
<td>(c)</td>
</tr>
<tr>
<td></td>
<td>(d)</td>
</tr>
<tr>
<td></td>
<td>(e)</td>
</tr>
<tr>
<td></td>
<td>(f)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Currently held certificates in Zambia, if any, by applicant issued under the Electronic Communications and Transactions Act, 2009</th>
<th>Certificate/Accreditation (Type and No.)</th>
<th>Nature of Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>(a)</td>
<td>(a)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b)</td>
<td>(b)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(c)</td>
<td>(c)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(d)</td>
<td>(d)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(e)</td>
<td>(e)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(f)</td>
<td>(f)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Currently held certificates in Zambia, if any, by subsidiary companies issued under the Electronic Communications and Transactions Act, 2009</th>
<th>Certificate/Accreditation (Type and No.)</th>
<th>Nature of Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>(a)</td>
<td>(a)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b)</td>
<td>(b)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(c)</td>
<td>(c)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(d)</td>
<td>(d)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(e)</td>
<td>(e)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(f)</td>
<td>(f)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Expiry date of certificate/accreditation in respect of which this application is made</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Have you been convicted of an offence involving fraud or dishonesty or of any offence under the Electronic Communications and Transactions Act, 2009, or any other law within or outside Zambia?</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>If yes, specify details:</td>
</tr>
<tr>
<td></td>
<td>Nature of offence:</td>
</tr>
<tr>
<td></td>
<td>Date of Conviction:</td>
</tr>
<tr>
<td></td>
<td>Sentence:</td>
</tr>
</tbody>
</table>
11. Have you ever applied to provide cryptography services in Zambia?
If yes please give details:

<table>
<thead>
<tr>
<th>Service applied for</th>
<th>Location</th>
<th>Brief description of service</th>
<th>Date of application</th>
<th>Status of application (Granted, rejected or pending)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* If application was rejected, give reasons for rejection:

12. Appendices

- **Appendix No. 1** Service design (including spectrum requirements, where applicable), rollout plan and implementation schedule including coverage area and intended performance levels

- **Appendix No. 2** Technical specifications for interoperability and compatibility of the cryptography service with other systems including but not limited to those owned and operated by electronic communications service licensees

- **Appendix No. 3** Business plan for proposed services (Should include information on technical proposal of the services to be provided, information on previous experience in the provision of the services, the profile of the individual, company or partnership, as the case may be)

- **Appendix No. 4** Investment certificate issued by the Zambia Development Agency, where applicable

- **Appendix No. 5** Certified photocopies of work permits and other relevant permits issued by the Immigration Department (where applicable)

- **Appendix No. 6** Tax Payers Identification Number (TPIN)

13. **QUALITY OF SERVICE UNDERTAKING**

I/we declare that the quality of service I/we provide shall meet the minimum requirements set out under the Act or any other law or, guidelines published by the Authority or any international standard.
14. DECLARATION
I/we declare that all the particulars and information provided in this application are complete, correct and true and I/we agree that in the event that any of the said particulars and information provided is found to be untrue or fraudulent, the certificate/accreditation will be revoked.
I/we agree that in the event of the revocation of the certificate/accreditation, any fee paid to the Authority shall be forfeited.
I/we declare that in the event that the nature of my/our business changes, or I/we no longer carry out operations in terms of the certificate/accreditation.
I/we will notify the Authority in which case my/our certificate/accreditation may be revoked or revised.
Declared at ............... this .................... day of .................... 20 ........... by the following persons who are duly authorised to sign for and on behalf of the applicant under the authority of the Power of Attorney or Board Resolution which is hereby attached.

Applicant's name ___________________________ Date ____________

Applicant's signature ___________________________

FOR OFFICIAL USE ONLY
Received by: ___________________________ Officer
Date Received ___________________________
Amount Received ___________________________
Serial No. of application: ___________________________
NOTICE OF INTENTION TO SUSPEND OR REVOKE CERTIFICATE OF REGISTRATION/ACCREDITATION

To (1) .................................................................................................................................

IN THE MATTER OF (2) .................................................................................................
you are hereby notified that the Authority intends to *suspend/cancel your* certificate/accreditation on the following grounds:
(a) ........................................................................................................................................
(b) ........................................................................................................................................
(c) ........................................................................................................................................
(d) ........................................................................................................................................

You are requested to appear before me on the ...... day of .......... 20 .......... at the Zambia Information and Communications Technology Authority, Lusaka, to show cause why your certificate/accreditation should not be rejected/take remedial measures to address the concerns raised in paragraphs ...... above before the ...... day of ...... 20 ......

If you fail to *appear before me/take the necessary remedial measures before the stipulated date, your certificate/accreditation will be suspended and subsequently revoked.

Accordingly, you are requested to take action to remedy the breaches set out in paragraphs ...... (above) within ...... days of receiving this notice. Failure to remedy the said breaches shall result in the *suspension/cancellation of your certificate/accreditation.

Dated this ...... day of .......... 20 ...........

(4) .................................................................................................................................

Director-General

*Delete as appropriate

OFFICIAL USE ONLY

This notice has, this ...... day of .......... 20 ........,
been entered in the Register

.........................................................

Director-General
NOTICE OF SUSPENSION OR REVOCATION OF CERTIFICATE OF REGISTRATION/ACCREDITATION

To (1).................................................................................................................................................................

...........................................................................................................................................................................

IN THE MATTER OF (2)................................................................you are hereby notified that your certificate of registration/accrreditatation has been suspended/revoked on the following grounds:

(a)..............................................................................................................................................................................

(b)..............................................................................................................................................................................

(c)..............................................................................................................................................................................

(d)..............................................................................................................................................................................

Dated this .......... day of ......... 20......................................................................................................................

(3) ................................................

Director-General

*Delete as appropriate

FOR OFFICIAL USE ONLYT
his notice has, this ..................... day of .......... 20............, been entered in the Register

..........................................................

Director-General
SECOND SCHEDULE
(Regulation 56)

PREScribed FEES

<table>
<thead>
<tr>
<th>Item</th>
<th>Fee Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Application for registration/accreditation</td>
<td>55,556</td>
</tr>
<tr>
<td>2. Application for variation of nature of cryptography/ authentication service</td>
<td>55,556</td>
</tr>
<tr>
<td>3. Notice of discontinuation of cryptography/authentication service</td>
<td>55,556</td>
</tr>
<tr>
<td>4. Assignment, ceding or transfer of certificate of accreditation registration/</td>
<td>55,556</td>
</tr>
<tr>
<td>5. Application for renewal of certificate of registration/accreditation</td>
<td>55,556</td>
</tr>
</tbody>
</table>

 **PROF. G. LUNGWANGWA,**

 *Minister of Communications and Transport*

LUSAKA

4th July, 2011

[MCT/64/1/1]