

LEGAL NOTICE NO.

THE KENYA INFORMATION AND COMMUNICATIONS ACT
(Cap. 411A)

**THE KENYA INFORMATION AND COMMUNICATIONS (ELECTRONIC
CERTIFICATION) REGULATIONS, 2026**

ARRANGEMENT OF REGULATIONS

Regulation

PART I—PRELIMINARY

- 1—Citation
- 2—Interpretation
- 3—Objects of the Regulations
- 4—Application

PART II—LICENSING OF ELECTRONIC CERTIFICATION SERVICE PROVIDERS

- 5—Application for a licence
- 6—Duration and renewal of licences
- 7—Digital signature scheme
- 8—Storage of private keys
- 9—Disposal of key pairs

**PART III—RECOGNITION OF FOREIGN ELECTRONIC CERTIFICATION SERVICE
PROVIDERS**

- 10—Criteria for recognition
- 11—Application for recognition
- 12—Grant and effect of recognition
- 13—Revocation of recognition

PART IV—OBLIGATIONS OF ELECTRONIC CERTIFICATION SERVICE PROVIDERS

- 14—Certificate policy and certification practice statement
- 15—Responsibilities of electronic certification service providers
- 16—Records management
- 17—Issue of certificates
- 18—Liability of electronic certification service providers
- 19—Renewal of certificates
- 20—Suspension of certificates
- 21—Revocation of certificates
- 22—Security procedures
- 23—Incident handling
- 24—Confidentiality

25—Winding up of operations

PART V—GENERAL PROVISIONS

26—Obligations of subscribers

27—Register of electronic certification service providers

28—Performance audits

29—Sanctions

30—Application of the General Licensing Regulations

31—Revocation

32—Savings and transitional provisions

THE KENYA INFORMATION AND COMMUNICATIONS ACT
(Cap. 411A)

IN EXERCISE of the powers conferred by section 83R of the Kenya Information and Communications Act, the Cabinet Secretary for Information, Communications and the Digital Economy makes the following Regulations—

**THE KENYA INFORMATION AND COMMUNICATIONS (ELECTRONIC
CERTIFICATION) REGULATIONS, 2026**

PART I—PRELIMINARY

Citation.

1. These Regulations may be cited as the Kenya Information and Communications (Electronic Certification) Regulations, 2026.

Interpretation.

Cap. 411A.

2. In these Regulations, unless the context otherwise requires—

“Act” means the Kenya Information and Communications Act;

“Authority” means the Communications Authority of Kenya established under section 3 of the Act;

“certificate” or “digital certificate” means a digital representation of information, or a set of data or record, issued by an electronic certification service provider for the purpose of supporting a digital signature, which—

- (a) authenticates the identity or other significant characteristics of the person who holds a particular key pair;
- (b) names or identifies the person to whom it is issued;
- (c) contains the public key of the person to whom it is issued;
- (d) identifies its period of validity; and
- (e) is digitally signed by the electronic certification service provider issuing it;

“certificate policy” means a document setting out the rules governing the applicability of a digital certificate to a particular community or class of applications with common security requirements;

“certification personnel” means a person who—

- (a) is responsible for the day-to-day operations, security and performance of an activity, relating to the provision of electronic certification services, regulated under the Act and these Regulations; or
- (b) has duties which directly involve the issue, renewal, suspension or revocation of certificates, the creation of private keys or the administration of the computing facilities of an electronic certification service provider;

“certification practice statement” means a document stating the practices which an electronic certification service provider employs in approving or rejecting certificate applications, or in issuing, managing or revoking certificates;

“digital signature” means an electronic signature created by the transformation of a message using an asymmetric cryptosystem and a hash function, such that a person having the original message and the signer’s public key can determine—

- (a) whether the transformation was created using the private key which corresponds to the signer’s public key;
- (b) whether the message has been altered since the transformation was made; and
- (c) whether the signature is capable of identifying the signatory;

“electronic certification service provider” means a person licensed under the Act to provide electronic certification services, and includes a recognised foreign electronic certification service provider;

“foreign electronic certification service provider” means a person authorised to provide electronic certification services outside Kenya who is recognised under regulation 12;

“key” means a mathematically related value used in a cryptographic process;

“key pair” means a private key and its corresponding public key, which are mathematically related for use in an asymmetric cryptosystem;

“licensee” means a person licensed under the Act to issue digital certificates;

“private key” means the secret key of a key pair, used to create a digital signature;

“public key” means the publicly available key of a key pair, used to verify a digital signature;

“repository” means a system for storing and retrieving certificates and other information relevant to certificates, including notices of the suspension or revocation of certificates;

“subscriber” means a person to whom a certificate is issued by an electronic certification service provider, and includes a person named or identified in a certificate as the holder of the key pair to which the certificate relates; and

“Tribunal” means the Communications and Multimedia Appeals Tribunal established under section 102 of the Act.

Objects of the Regulations.

3. The objects of these Regulations are to—

- (a) provide a framework for the licensing, administration and regulation of electronic certification service providers;
- (b) provide for the recognition of foreign electronic certification service providers;

- (c) promote trust, reliability, integrity and security in electronic certification services and digital signatures; and
- (d) protect subscribers and persons who reasonably rely on digital certificates.

Application.

4. These Regulations apply to the provision of electronic certification services in Kenya, to subscribers and to persons who rely on certificates issued under these Regulations.

PART II—LICENSING OF ELECTRONIC CERTIFICATION SERVICE PROVIDERS

Application for a licence.

5. (1) A person intending to provide electronic certification services shall apply to the Authority for a licence in accordance with the Act and in a manner set out under the regulations relating to the general licensing and shall pay the prescribed fee.

(2) An application under sub-regulation (1) shall be accompanied by—

- (a) the proposed digital signature scheme, certificate policy and certification practice statement; and
- (c) any other relevant information reasonably required in the circumstances for the purposes of determining the application.

(3) The Authority shall process the application in a manner provided for under the regulations relating to general licensing.

Duration and renewal of licences.

6. (1) An electronic certification service provider's licence is valid for a period of fifteen years.

(2) The procedure for the renewal of the licence is that set out in the regulations relating to general licensing made under the Act.

Digital signature scheme.

7. (1) An electronic certification service provider shall not commence operations unless its digital signature scheme has been approved by the Authority.

(2) In considering the approval of a digital signature scheme, the Authority shall take into account whether—

- (a) the scheme uses a secure public-key algorithm for the generation of the key pair, and a secure public-key algorithm and hash function for the creation of the digital signature;
- (b) the scheme satisfies the technical component requirements; and
- (c) a digital signature created under the scheme is not capable of being modified to contain a subliminal channel.

(3) A licensee shall ensure that its cryptographic key management practices appropriately separate the signature and encryption functions, where necessary to preserve the integrity, security and reliability of digital signatures.

Storage of private keys.

8. (1) A licensee shall specify the data storage medium for private keys, which may be hardware-based or software-based.

(2) Where the data storage medium of a private key is—

(a) hardware-based, the holder of the private key shall ensure that the token, smart card or other external device in which the private key is stored is kept in a secure manner and place; and

(b) software-based, the holder of the private key shall ensure that the computer system in which the private key is stored is reasonably secure.

(3) The personal identification numbers, passwords or other credentials used for access to a private key, together with the data storage medium for the private key, shall be kept secret and protected against unauthorised disclosure.

Disposal of key pairs.

9. (1) Where a key pair is no longer in use or intended to be used, or the private key of the key pair is compromised, the holder of the key pair shall dispose of it in a secure manner.

(2) Secure disposal under sub-regulation (1) may include destruction or any other method which ensures that the private key cannot be recovered or used.

(3) Despite sub-regulation (1), where the holder intends to retain a key pair which is no longer in use or intended to be used, or which has been compromised, the holder shall ensure that the key pair is stored in a reasonably secure manner and is not used for any electronic certification purpose.

PART III—RECOGNITION OF FOREIGN ELECTRONIC CERTIFICATION SERVICE PROVIDERS

Criteria for recognition.

10. The Authority may recognise a foreign electronic certification service provider for the purposes of these Regulations where the provider—

(a) is duly licensed or authorised by a competent authority to provide electronic certification services in the country of origin;

(b) demonstrates compliance with requirements equivalent to those prescribed under the Act and these Regulations, including the applicable technical and security standards; and

(c) has established a local presence in Kenya, including a duly appointed local agent.

Application for recognition.

11. (1) A foreign electronic certification service provider seeking recognition shall apply to the Authority in the manner specified in the general licensing regulations, and shall pay the prescribed fee.

(2) An application under sub-regulation (1) shall be accompanied by—

(a) proof of authorisation or licensing in the country of origin;

(b) a report from a qualified independent auditor confirming compliance with the applicable technical, security and operational standards;

(c) details of the applicant's certificate policy and certification practice statement; and

(d) any relevant due diligence information or document which the Authority may require to evaluate the application.

(3) The procedure for the determination of an application under this regulation, the imposition of conditions, the giving of reasons and the review of, and appeal against, a decision of the Authority is that set out in the regulations relating to general licensing.

Grant and effect of recognition.

12. (1) A foreign electronic certification service provider recognised under these Regulations shall be treated as an electronic certification service provider for the purposes of the Act and these Regulations.

(2) Recognition shall be evidenced by a certificate of recognition issued by the Authority.

(3) A recognised foreign electronic certification service provider shall comply with the conditions of the recognition and the applicable provisions of these Regulations.

Revocation of recognition.

13. (1) The Authority may revoke the certificate of recognition of a foreign electronic certification service provider where the provider—

- (a) no longer satisfies the requirements specified under the Act or these Regulations;
- (b) contravenes the Act, these Regulations or a condition of the recognition; or
- (c) requests the revocation of the recognition, in writing.

(2) A revocation under this regulation shall be published on the website of the Authority and in the Gazette.

(3) A revocation under this regulation does not preclude the foreign electronic certification service provider from making a new application for recognition.

PART IV—OBLIGATIONS OF ELECTRONIC CERTIFICATION SERVICE PROVIDERS

Certificate policy and certification practice statement.

14. (1) An electronic certification service provider shall develop and maintain—

- (a) a certificate policy; and
- (b) a certification practice statement.

(2) A certificate policy and a certification practice statement shall specify—

- (a) the rules governing the use of certificates;
- (b) the subscriber identity verification procedures;
- (c) the procedures for the issue, renewal, suspension and revocation of certificates;
- (d) the security controls and operational procedures; and
- (e) any limitation of liability and any reliance conditions.

(3) An electronic certification service provider shall file its certificate policy and certification practice statement with the Authority, and shall publish them in a manner accessible to the public.

(4) An electronic certification service provider shall not change its certificate policy or certification practice statement without the prior written approval of the Authority.

(5) An electronic certification service provider shall log all the changes to its certificate policy and certification practice statement, and shall specify the effective date of each change.

(6) An electronic certification service provider shall keep, in a secure manner, a record of each version of its certificate policy and certification practice statement, and shall record the date on which each version came into effect and the date on which it ceased to have effect.

Responsibilities of
electronic certification
service providers.

15. An electronic certification service provider shall—

- (a) issue and renew certificates;
- (b) suspend or revoke certificates;
- (c) verify the identity of subscribers;
- (d) publish accurate and up-to-date information relating to certificates;
- (e) maintain a repository service listing all the published certificates, and the records of revoked certificates, which may be used to verify the validity of published certificates;
- (f) ensure the integrity, confidentiality and security of its systems and operations; and
- (g) provide time-stamping or related trust services, where applicable.

Records management.

16. (1) An electronic certification service provider shall keep securely all the records relating to—

- (a) the issue, renewal, suspension or revocation of certificates, including the identity of any person requesting a certificate;
- (b) the process of the generation of key pairs by the subscribers or by the electronic certification service provider; and
- (c) the administration of its computing facilities.

(2) An electronic certification service provider shall keep its records in electronic and print form, and shall avail the records to the Authority on request.

(3) An electronic certification service provider shall—

- (a) index, store and preserve the records kept under sub-regulation (1) in a form in which the records may be reproduced in a legible, accurate and complete manner accessible to the Authority or its appointed agents; and

- (b) retain all the records required to be kept, and all the logs of the creation of the archive of certificates required under this regulation, for a period of not less than seven years.

Issue of certificates.

17. (1) An electronic certification service provider shall issue a certificate to a subscriber only after verifying the identity of the subscriber in accordance with its certificate policy and certification practice statement.

(2) A certificate shall contain—

- (a) the identification of the electronic certification service provider;
- (b) the identification of the subscriber;
- (c) the period of validity of the certificate;
- (d) information regarding the authorisation of the subscriber, where the subscriber is acting on behalf of another person;
- (e) information regarding the conditions of use of the certificate and the limits on the value of transactions, where applicable;
- (f) the secure digital signature of the electronic certification service provider, which verifies the information in the certificate;
- (g) information sufficient to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate will be listed, if the certificate is suspended or revoked; and
- (h) any other relevant information.

(3) An electronic certification service provider shall—

- (a) give a subscriber an opportunity to verify the contents of the certificate before the subscriber accepts it;
- (b) inform a subscriber, in writing, of the legal effect of a digital signature, the limitations on the use of certificates and the applicable dispute resolution procedures; and
- (c) notify subscribers, in writing, not to allow third parties to use the signature creation data associated with the signature verification data in the certificate.

(4) Where a subscriber accepts an issued certificate, the electronic certification service provider shall publish a signed copy of the certificate in a repository.

(5) Where a subscriber does not accept a certificate, the electronic certification service provider shall not publish the certificate.

(6) Where a certificate has been issued by an electronic certification service provider and accepted by the subscriber, the electronic certification service provider shall notify the subscriber, within three working days, of any fact which subsequently becomes known to the provider and which may significantly affect the validity or reliability of the certificate.

(7) An electronic certification service provider shall log, and keep in a secure manner, the date and time of all the transactions relating to the issue of a certificate.

(8) Where an electronic certification service provider issues an additional certificate to a person on the basis of a valid certificate held by the same person, and the original certificate is subsequently suspended or revoked, the electronic certification service provider shall investigate and determine whether the additional certificate should be suspended or revoked.

Liability of electronic certification service providers.

18. (1) An electronic certification service provider, by issuing or guaranteeing a certificate to the public, accepts liability for damage caused to a person who reasonably relies on the certificate, unless the electronic certification service provider proves that it was not negligent.

(2) The liability of an electronic certification service provider under sub-regulation (1) relates to—

- (a) the accuracy, at the time of the issue of the certificate, of all the information contained in the certificate, and the fact that the certificate contains all the details required for the certificate;
- (b) the assurance that, at the time of the issue of the certificate, the signatory identified in the certificate held the signature creation data corresponding to the signature verification data given or identified in the certificate;
- (c) the assurance that the signature creation data and the signature verification data can be used in a complementary manner, where the electronic certification service provider generated both of them; and
- (d) the failure to publish a notice of the suspension or revocation of a certificate in the repository specified in the certificate.

(3) Where an electronic certification service provider has specified in a certificate the limits on the use of the certificate and the limits on the value of the transactions for which the certificate may be used, the provider shall put in place mechanisms to revoke the validity of the subscriber's certificate, and is not liable for damage resulting from use exceeding those limits.

Renewal of certificates.

19. (1) An electronic certification service provider shall renew certificates in accordance with the identity verification procedures specified in its certificate policy and certification practice statement.

(2) An electronic certification service provider shall maintain the records of all certificate renewal transactions.

Suspension of certificates.

20. (1) An electronic certification service provider shall maintain facilities capable of receiving and responding to requests for the suspension of certificates on a continuous basis.

(2) An electronic certification service provider shall suspend a certificate—

- (a) on receipt of a valid request by the subscriber or an authorised agent of the subscriber; or

(b) where it has reasonable grounds to believe that the certificate is unreliable or that the corresponding private key may have been compromised.

(3) A suspension under this regulation is temporary, and remains in force until the certificate is reinstated or revoked.

(4) An electronic certification service provider shall, without undue delay, publish notice of the suspension in the relevant repository and notify the subscriber.

(5) The subscriber identity verification method employed for the suspension of certificates shall be specified in the certificate policy and certification practice statement.

(6) An electronic certification service provider shall, after such inquiry as may be necessary, determine whether a suspended certificate should be reinstated or revoked, and shall record the date and time of all suspension-related transactions.

Revocation of
certificates.

21. (1) An electronic certification service provider shall revoke a certificate where—

- (a) it receives a request for revocation from the subscriber or an authorised agent of the subscriber;
- (b) the information contained in the certificate is no longer accurate or reliable;
- (c) the certificate was issued on the basis of false, misleading or fraudulent information; or
- (d) the subscriber becomes bankrupt or incapacitated, or dies.

(2) The subscriber identity verification method employed for the revocation of certificates shall be specified in the certificate policy and certification practice statement.

(3) An electronic certification service provider shall, without undue delay, publish notice of the revocation in the relevant repository and notify the subscriber or the authorised agent.

(4) An electronic certification service provider shall log, and keep in a secure manner, the date and time of all the transactions relating to the revocation of a certificate.

(5) A person who wishes to rely on a certificate shall, before relying on the certificate, establish the status of the certificate from the electronic certification service provider.

Security procedures.

22. (1) An electronic certification service provider shall provide every subscriber with a secure and trustworthy system for the generation of the subscriber's key pair.

(2) An electronic certification service provider shall establish a mechanism which generates and verifies digital signatures in a secure and trustworthy manner and which indicates the validity of a digital signature.

(3) Where a digital signature is not valid, the mechanism established under sub-regulation (2) shall provide the reason for the invalidity and the status of the certificate.

(4) Where a verification mechanism is established by a person who is not an electronic certification service provider, a signature resulting from the mechanism shall not be considered secure unless an electronic certification service provider endorses the implementation of the mechanism and its certificate.

(5) An electronic certification service provider shall store the keys, including the subscriber's keys and the provider's own keys, in a secure and trustworthy manner.

(6) An electronic certification service provider shall, in addition to its internal security procedures, comply with the security procedures issued by the Authority.

Incident handling.

23. (1) An electronic certification service provider shall establish an incident management plan to address incidents relating to—

- (a) the compromise of keys;
- (b) the penetration of the systems and networks of the electronic certification service provider;
- (c) the unavailability of infrastructure; and
- (d) the fraudulent registration and generation of certificates, and of certificate suspension and revocation information.

(2) Where an incident contemplated under sub-regulation (1) occurs, the electronic certification service provider shall report the incident to the Authority within twenty-four hours.

Confidentiality.
Cap. 411C.

24. (1) An electronic certification service provider shall not collect personal data directly from subscribers or their authorised agents unless the personal data is necessary for the purposes of the issue of a certificate and the collection is consistent with the provisions of the Data Protection Act.

(2) An electronic certification service provider shall keep all the information relating to a subscriber confidential.

(3) An electronic certification service provider shall not disclose or share information relating to a subscriber except on a lawful basis or pursuant to an order of a court.

(4) The obligation of confidentiality under sub-regulation (3) does not apply to information relating to a subscriber which—

- (a) is contained in the certificate and is available to the public for inspection;
- (b) is otherwise provided by the subscriber to the electronic certification service provider for disclosure to the public; or
- (c) relates to the revocation or suspension of a certificate.

Winding up of operations.

(5) Where an electronic certification service provider has permitted a subscriber to use a pseudonym, the provider shall, at the request of a law enforcement authority, disclose the data relating to the subscriber which is required for the prosecution of offences.

25. (1) An electronic certification service provider shall not discontinue its operations without the approval of the Authority.

(2) An electronic certification service provider which intends to discontinue its operations shall—

- (a) give the Authority and its subscribers a minimum of six months' notice, in writing, of its intention to discontinue its operations; and
- (b) publish its intention to discontinue its operations in at least two local daily newspapers of nationwide circulation, and in such other manner as the Authority may determine.

(3) In addition, an electronic certification service provider which intends to discontinue its operations shall—

- (a) arrange for its subscribers to re-subscribe to, or to be on-boarded by, another licensed electronic certification service provider;
- (b) make arrangements for its records and certificates to be archived in a secure manner; and
- (c) with the written approval of the Authority, transfer its records to another electronic certification service provider in a secure manner.

(4) An electronic certification service provider which contravenes this regulation commits an offence and is liable, on conviction, to a fine not exceeding one million shillings, or to imprisonment for a term not exceeding six months, or to both.

PART V—GENERAL PROVISIONS

Obligations of subscribers.

26. (1) Where a subscriber generates a key pair, the subscriber shall apply the relevant security procedures.

(2) A subscriber shall be treated as having accepted a certificate if the subscriber publishes, or authorises the publication of, the certificate to any person or in a repository, or otherwise demonstrates acceptance of the certificate.

(3) By accepting a certificate, the subscriber certifies, to every person who reasonably relies on the information contained in the certificate, that—

- (a) the subscriber holds, and is entitled to hold, the private key corresponding to the public key listed in the certificate;
- (b) all the representations made by the subscriber to the electronic certification service provider, and all the information contained in the certificate, are true; and

(c) all the information in the certificate is within the knowledge of the subscriber.

(4) A subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in the subscriber's certificate, and shall take the necessary steps to prevent its disclosure to a person who is not authorised to affix the digital signature of the subscriber.

(5) Where a subscriber becomes aware that a private key has been compromised, the subscriber shall notify the electronic certification service provider of the compromise within twenty-four hours.

Register of electronic certification service providers.

27. (1) The Authority shall establish and maintain a register of the electronic certification service providers licensed or recognised under these Regulations.

(2) The register shall contain—

- (a) the name and contact details of each licensee or recognised provider;
- (b) the status of the licence or recognition; and
- (c) any other relevant information.

(3) The Authority shall make the register publicly accessible on its website.

Performance audits.

28. (1) The Authority may conduct audits of the operations of a licensee to assess compliance with the Act, these Regulations and the conditions of the licence.

(2) A licensee shall—

- (a) provide the information, records and access reasonably required for the purposes of an audit; and
- (b) cooperate with the Authority, or its authorised agents, in the conduct of the audit.

(3) The Authority may issue directions to a licensee arising from the findings of an audit.

Sanctions.

29. (1) Where a licensee contravenes these Regulations or a condition of a licence, the Authority may impose administrative sanctions, including—

- (a) the issue of a warning or a directive;
- (b) the suspension of the licence; or
- (c) the revocation of the licence.

(2) Before imposing a sanction under sub-regulation (1), the Authority shall give the licensee an opportunity to be heard.

(3) The imposition of an administrative sanction does not preclude the institution of criminal proceedings where an offence is disclosed.

Application of the General Licensing Regulations.

30. The regulations relating to general licensing made under the Act apply, with the necessary modifications, to any matter concerning a licence under these Regulations for which these Regulations do not otherwise provide.

Revocation.
L.N. No. 116 of 2010.

31. The Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations, 2010 are revoked.

Savings and
transitional provisions.

32. (1) Despite the revocation under regulation 31—

- (a) proceedings, approvals and decisions subsisting immediately before the commencement of these Regulations continue as if made under these Regulations;
- (b) rights, obligations and liabilities accrued under the revoked Regulations continue to be enforceable; and
- (c) a period of time running under the revoked Regulations continues to run as if these Regulations had been in force at the time the period began.

(2) A licence issued before the commencement of these Regulations continues in force in accordance with its terms, subject to these Regulations.

(3) An existing electronic certification service provider shall, within the period specified by the Authority, comply with these Regulations.

Made on the, 2026.

WILLIAM KABOGO GITAU,
Cabinet Secretary for Information, Communications and the Digital Economy.